Cisco IP Phone 8811, 8841, 8851, and 8861 Administration Guide for Cisco Unified Communications Manager 10.5

First Published: September 05, 2014

Last Modified: March 16, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xiii

Overview xiii

Audience xiii

Guide Conventions xiii

Related Documentation xv

Cisco IP Phone 8800 Series Documentation xv

Cisco Unified Communications Manager Documentation xv

Cisco Business Edition 3000 Documentation xv

Cisco Business Edition 6000 Documentation xv

Documentation, Support, and Security Guidelines xv

Cisco Product Security Overview xvi

PART I About the Cisco IP Phone 1

CHAPTER 1 Technical Details 3

Physical and Operating Environment Specifications 3

Cable Specifications 4

Network and Computer Port Pinouts 4

Network Port Connector 5

Computer Port Connector 5

Phone Power Requirements 6

Power Outage 7

Power Reduction 7

Power Negotiation Over LLDP 8

Network Protocols 8

VLAN Interaction 13

Cisco Unified Communications Manager Interaction 13

Cisco Unified Communications Manager Express Interaction 14
Voice Messaging System Interaction 14
Phone Startup Overview 15
External Devices 16
USB Port Information 17
Phone Configuration Files 17

CHAPTER 2 Cisco IP Phone Hardware 19
Phone Overview 19
Cisco IP Phone 8811 20
Phone Connections 20
Buttons and Hardware 22
Cisco IP Phone 8841 25
Phone Connections 25
Buttons and Hardware 26
Cisco IP Phone 8851 29
Phone Connections 29
Buttons and Hardware 30
Cisco IP Phone 8861 33
Phone Connections 33
Buttons and Hardware 35
Terminology Differences 38

PART II Cisco IP Phone Installation 39

CHAPTER 3 Cisco IP Phone Installation 41
Verify Network Setup 41
Enable Autoregistration for Phone 42
Install Cisco IP Phone 43
Set Up Phone from Setup Menus 44
Apply Phone Password 45
Text Menu Entry from Phone 46
Set Up Wireless LAN 46
Set Up Wireless LAN from Cisco Unified Communications Manager 47
Set Up Wireless LAN from Phone 48

Configure Network Settings 51
Set Up IPv4 54
Set Up IPv6 57
Set Domain Name Field 60
Set Admin VLAN ID Field 60
Set PC VLAN Field 60
Set SW Port Setup Field 60
Set PC Port Setup Field 61
Set Wireless Field 61
Set WLAN Sign In Access Field 61
Set SSID Field 61
Set Security Mode Field 62
Set 802.11 Mode Field 62
Set DHCP Enabled Field 62
Set IP Address Field 62
Set Subnet Mask Field 63
Set Default Router Field 63
Set DNS Server Fields 63
Set Alternate TFTP Field 63
Set TFTP Server 1 Field 64
Set TFTP Server 2 Field 64
Set Up Phone to Use DHCP 64
Set Up Phone to Not Use DHCP 65
Phone Startup Verification 65
Configure Phone Services for Users 65

CHAPTER 4 **Cisco Unified Communications Manager Phone Setup 67**
Set Up Cisco IP Phone 67
Determine Phone MAC Address 70
Phone Addition Methods 71
Add Phones Individually 71
Add Phones Using BAT Phone Template 71
Add Users to Cisco Unified Communications Manager 72
Add a User from an External LDAP Directory 73
Add User Directly to Cisco Unified Communications Manager 73

Add User to End User Group 74
Associate Phones with Users 74
Survivable Remote Site Telephony 75
Set Up Cisco Unified Communications Manager Features 77

CHAPTER 5 Self Care Portal Management 79
Self Care Portal Overview 79
Set Up Access to Self Care Portal 80
Customize Self Care Portal Display 80

PART III Hardware and Accessory Installation 81

CHAPTER 6 Cisco IP Phone Accessories 83
Accessory Support 83
Connect Footstand 84
Secure the Phone with a Cable Lock 84
External Speakers and Microphone 85
Headsets 85
Audio Quality 86
Analog Headsets 86
Enable Wideband on Analog Headsets 86
Enable Wideband Codec on Analog Headsets 86
Wired Headsets 87
Connect Wired Headset 87
Disable Wired Headset 87
USB Headsets 88
Enable USB Headset 88
Disable USB Headset 88
Wireless Headsets 89
Enable Electronic Hookswitch 89
Bluetooth Wireless Headsets 89
Enable Bluetooth Wireless Headset 91

CHAPTER 7 Cisco IP Phone Key Expansion Module 93
Cisco IP Phone Key Expansion Module Setup Overview 93

KEM Power Information 94
Connect Single KEM to Cisco IP Phone 95
Connect Two or Three KEMs to Cisco IP Phone 99
Set Up Key Expansion Module in Cisco Unified Communications Manager Administration 103
Access Key Expansion Module Setup 105
Reset Key Expansion Module 106
Troubleshoot the Key Expansion Module 106

CHAPTER 8 Wall Mounts 109
Wall Mount Options 109
Non-Lockable Wall Mount Components for Phone 109
Install the Non-Lockable Wall Mount Kit for Phone 111
Remove the Phone from the Non-Lockable Wall Mount 115
Non-Lockable Wall Mount Components for Phone with Key Expansion Module 116
Install Non-Lockable Wall Mount Kit for Phone with Key Expansion Module 118
Remove the Phone and Key Expansion Module from the Non-Lockable Wall Mount 121
Adjust the Handset Rest 122

PART IV Cisco IP Phone Administration 125

CHAPTER 9 Cisco IP Phone Security 127
View Current Security Features on Phone 127
View Security Profiles 127
Supported Security Features 128
Set Up Locally Significant Certificate 132
Phone Call Security 133
Secure Conference Call Identification 134
Secure Phone Call Identification 135
Provide Encryption for Barge 136
WLAN Security 136
802.1X Authentication 139
Access 802.1X Authentication 140
802.1X Authentication Options 141
Set Device Authentication Field 142

CHAPTER 10 Cisco IP Phone Customization 143

Custom Phone Rings 143

Set Up Custom Phone Rings 143

Custom Ring File Formats 144

Custom Background Images 145

Set Up Custom Background Image 145

Custom Background File Formats 146

Set Up Wideband Codec 147

Set Up Idle Display 148

CHAPTER 11 Phone Features and Setup 151

Phone Features and Setup Overview 152

Cisco IP Phone User Support 152

Telephony Features 153

Feature Buttons and Softkeys 171

Disable Speakerphone 173

Schedule Power Save for Cisco IP Phone 173

Schedule Power Save Plus (EnergyWise) on Cisco IP Phone 174

Enable Agent Greeting 177

Set Up the DF Bit 178

Set Up Do Not Disturb 178

Set Up Monitoring and Recording 179

Set Up Power Negotiation for LLDP 180

Set Up Bluetooth Profiles 180

Set Up Automatic Port Synchronization 181

Set Up SSH Access 181

Set Up Call Forward Notification 182

Set Up Client Matter Codes 183

Enable BLF for Call Lists 183

Set Up Dual Bank Information 184

Set Up Forced Authorization Codes 184

Set Up Incoming Call Toast Timer 185

Set Up Peer Firmware Sharing 185

Set Up Remote Port Configuration 186

Set Headset Sidetone Control 187
Enable Device Invoked Recording 188
Set Up Dial Tone from Release Button 188
Park Monitoring 189
Set Up Park Monitoring Timers 189
Set Park Monitoring Parameters for Directory Numbers 190
Set Up Park Monitoring for Hunt Lists 191
Enable Actionable Incoming Call Alert 191
Enable the Call History Display Enhancement 192
Enable Call History for Shared Line 193
Set Up the Default Line Filter 193
Set Up Custom Line Filter 193
Phone Button Templates 194
Modify Phone Button Template 194
Assign Phone Button Template for All Calls 195
Set Up PAB or Speed Dial as IP Phone Service 195
Modify Phone Button Template for PAB or Fast Dial 196
Control Phone Web Page Access 197
Set Up Softkey Template 198
Set Up RTP/sRTP Port Range 200
Set Up TLS Resumption Timer 201
Set Up Visual Voicemail 202
Set Up Visual Voicemail for a Specific User 203
Visual Voicemail Setup for a User Group 203
Enable Intelligent Proximity 203
Manage Join Across Lines and Transfer Across Lines 204

CHAPTER 12 **Corporate and Personal Directory** 205
Corporate Directory Setup 205
Personal Directory Setup 205
User Personal Directory Entries Setup 206
Download Cisco IP Phone Address Book Synchronizer 206
Cisco IP Phone Address Book Synchronizer Deployment 206
Install Synchronizer 207
Set Up Synchronizer 207

PART V Cisco IP Phone Troubleshooting 209

CHAPTER 13 Monitoring Phone Systems 211

Cisco IP Phone Status 211

Display Model Information Window 211

Model Information Fields 212

Display Status Menu 212

Display Status Messages Window 213

Status Messages Fields 213

Display Network Statistics Screen 220

Ethernet Statistics Information 220

Display Wireless Statistics Screen 224

WLAN Statistics 224

Display Call Statistics Window 225

Call Statistics Fields 226

Display Current Access Point Window 227

Current Access Points Fields 228

Cisco IP Phone Web Page 229

Access Web Page for Phone 230

Device Information 230

Network Setup 231

Network Statistics 236

Ethernet Information Web Page 236

Access and Network Web Pages 237

Device Logs 239

Streaming Statistics 239

Request Information from the Phone in XML 242

Sample CallInfo Output 243

Sample LineInfo Output 243

Sample ModeInfo Output 244

CHAPTER 14 Troubleshooting 245

General Troubleshooting Information 245

Startup Problems 247

Cisco IP Phone Does Not Go Through Normal Startup Process 247
Cisco IP Phone Does Not Register with Cisco Unified Communications Manager 248
Phone Displays Error Messages 248
Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager 248
Phone Cannot Connect to TFTP Server 248
Phone Cannot Connect to Server 249
Phone Cannot Connect Using DNS 249
Cisco Unified Communications Manager and TFTP Services Are Not Running 249
Configuration File Corruption 250
Cisco Unified Communications Manager Phone Registration 250
Cisco IP Phone Cannot Obtain IP Address 250
Cisco IP Phone Reset Problems 250
Phone Resets Due to Intermittent Network Outages 251
Phone Resets Due to DHCP Setting Errors 251
Phone Resets Due to Incorrect Static IP Address 251
Phone Resets During Heavy Network Usage 251
Phone Resets Intentional Reset 252
Phone Resets Due to DNS or Other Connectivity Issues 252
Phone Does Not Power Up 252
Phone Cannot Connect to LAN 253
Cisco IP Phone Security Problems 253
CTL File Problems 253
Authentication Error, Phone Cannot Authenticate CTL File 253
Phone Cannot Authenticate CTL File 253
CTL File Authenticates but Other Configuration Files Do Not Authenticate 254
ITL File Authenticates but Other Configuration Files Do Not Authenticate 254
TFTP Authorization Fails 254
Phone Does Not Register 254
Signed Configuration Files Are Not Requested 255
802.1X Authentication Problems 255
802.1X Enabled on Phone but Phone Does Not Authenticate 256
802.1X Not Enabled 256
Factory Reset of Phone Has Deleted 802.1X Shared Secret 257
General Telephone Call Problems 257

Phone Call Cannot Be Established 257
Phone Does Not Recognize DTMF Digits or Digits Are Delayed 258
Troubleshooting Procedures 258
Check TFTP Settings 258
Determine DNS or Connectivity Issues 259
Check DHCP Settings 259
Create New Phone Configuration File 260
Identify 802.1X Authentication Problems 261
Verify DNS Settings 261
Start Service 261
Additional Troubleshooting Information 262

CHAPTER 15 Maintenance 263
Basic Reset 263
Perform Factory Reset from Phone Keypad 264
Perform Factory Reset Phone Menu 264
Perform Network Configuration Reset 265
Perform User Network Configuration Reset 265
Remove CTL File 265
Quality Report Tool 266
Voice Quality Monitoring 266
Voice Quality Troubleshooting Tips 266
Cisco IP Phone Cleaning 267

CHAPTER 16 International User Support 269
Unified Communications Manager Endpoints Locale Installer 269
International Call Logging Support 269

Preface

- Overview, page xiii
- Audience, page xiii
- Guide Conventions, page xiii
- Related Documentation, page xv
- Documentation, Support, and Security Guidelines, page xv

Overview

The *Cisco Unified IP Phone 8811, 8841, 8851, and 8861 Administration Guide for Cisco Unified Communications Manager (SIP)* provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a VoIP network.

Because of the complexity of an IP telephony network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager or other network devices.

Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps that are required to set up Cisco IP phones. The tasks described in this document involve configuring network settings that are not intended for phone users. The tasks in this manual require a familiarity with Cisco Unified Communications Manager.

Guide Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.

Convention	Description
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
input font	Information you must enter is in input font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:

Attention IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

Use the following sections to obtain related information.

Cisco IP Phone 8800 Series Documentation

Refer to publications that are specific to your language, phone model, and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Business Edition 3000 Documentation

See the *Cisco Business Edition 3000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 3000 release. Navigate from the following documentation URL:

http://www.cisco.com/c/en/us/support/unified-communications/business-edition-3000/tsd-products-support-series-home.html

Cisco Business Edition 6000 Documentation

Refer to the *Cisco Business Edition 6000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 6000 release. Navigate from the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, reviewing security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

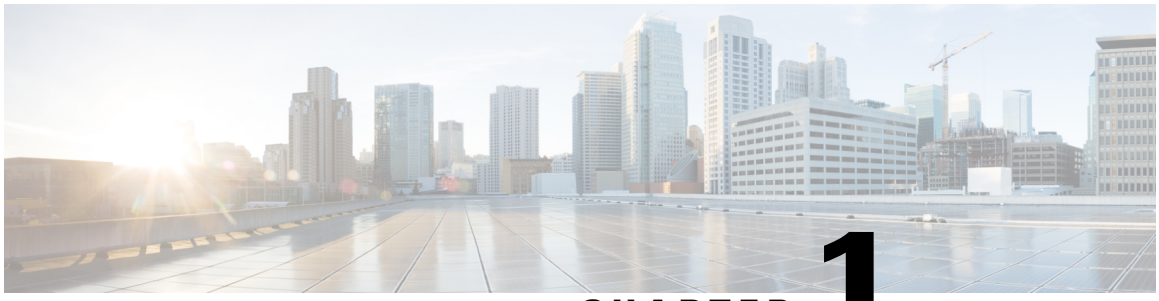
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.bis.doc.gov/policiesandregulations/ear/index.htm.

PART I

About the Cisco IP Phone

- Technical Details, page 3
- Cisco IP Phone Hardware, page 19



CHAPTER 1

Technical Details

- Physical and Operating Environment Specifications, page 3
- Cable Specifications, page 4
- Phone Power Requirements, page 6
- Network Protocols, page 8
- VLAN Interaction, page 13
- Cisco Unified Communications Manager Interaction, page 13
- Cisco Unified Communications Manager Express Interaction, page 14
- Voice Messaging System Interaction, page 14
- Phone Startup Overview, page 15
- External Devices, page 16
- USB Port Information, page 17
- Phone Configuration Files, page 17

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco IP Phones 8811, 8841, 8851, and 8861.

Table 1: Physical and Operating Specifications

Specification	Value or range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	Operating: 10% to 90% (non-condensing) Non-operating: 10% to 95% (non-condensing)
Storage temperature	14° to 140°F (–10° to 60°C)

Specification	Value or range
Height	9.02 in. (229.1 mm)
Width	10.13 in. (257.34 mm)
Depth	1.57 in. (40 mm)
Weight	2.62 lb (1.19 kg)
Power	100-240 VAC, 50-60 Hz, 0.5 A when using the AC adapter 48 VDC, 0.2 A when using the in-line power over the network cable
Cables	Category 3/5/5e/6 for 10-Mbps cables with 4 pairs Category 5/5e/6 for 100-Mbps cables with 4 pairs Category 5e/6 for 1000-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance requirements	As supported by the Ethernet Specification, the maximum cable length between each Cisco IP Phone and the switch is assumed to be 330 feet (100 meters).

Cable Specifications

The following information lists the cable specifications:

- RJ-9 jack (4-conductor) for handset and headset connection
- RJ-45 jack for the LAN 10/100/1000BaseT connection (10/100/1000 Network port on the phone)
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (10/100/1000 Computer port on the phone)
- 3.5 mm jack for speaker connection
- 48-volt power connector

Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The network port is the 10/100/1000 SW port on the Cisco IP Phone.
- The computer (access) port is the 10/100/1000 PC port on the Cisco IP Phone.

Network Port Connector

The following table describes the network port connector pinouts.

Table 2: Network Port Connector Pinouts

Pin number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Note BI stands for bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.	

Computer Port Connector

The following table describes the computer port connector pinouts.

Table 3: Computer (Access) Port Connector Pinouts

Pin number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+

Pin number	Function
8	BI_DC-

Note BI stands for bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.

Phone Power Requirements

The Cisco IP Phone can be powered with external power or with Power over Ethernet (PoE). A separate power supply provides external power. The switch can provide PoE through the phone Ethernet cable.

Note When you install a phone that is powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

The following table provides guidelines for Cisco IP Phone power.

Table 4: Guidelines for Cisco IP Phone Power

Power type	Guidelines
External power: Provided through the CP-PWR-CUBE-4= external power supply	The Cisco IP Phone uses the CP-PWR-CUBE-4 power supply.
External power—Provided through the Cisco IP Phone Power Injector.	The Cisco IP Phone Power Injector may be used with any Cisco IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco IP Phone Power Injector connects between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	Cisco IP Phone supports IEEE 802.3af Class 1 power on signal pairs and spare pairs. Cisco IP Phone supports IEEE 802.3af for external add-on devices. Cisco IP Phones 8851 and 8861 support IEEE 802.3af for smartphone charging. Cisco IP Phone 8861 supports IEEE 802.3at for tablet charging. To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information. Support for 802.3at: The Cisco IP Phone can draw more power than IEEE 802.3af, as long as there is 802.3at switch support.

For information about Cisco IP Phone 8800 Key Expansion Module power requirements, see KEM Power Information, on page 94.

The documents in the following table provide more information on the following topics:

- Cisco switches that work with Cisco IP Phones
- Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions about power

Document topics	URL
Cisco IP Phone Power Injector	http://www.cisco.com/en/US/products/ps6951/index.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/index.html
Cisco Catalyst Switches	http://www.cisco.com/en/US/products/hw/switches/index.html
Integrated Service Routers	http://www.cisco.com/en/US/products/hw/routers/index.html
Cisco IOS Software	http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Power Outage

Power outages and other devices can affect your Cisco IP Phone.

Your access to emergency service through the phone requires that the phone receive power. If a power interruption occurs, Service and Emergency Calling Service dialing will not function until power is restored. In case of a power failure or disruption, you may need to reset or reconfigure the equipment before you can use the Service or Emergency Calling Service dialing.

Power Reduction

You can reduce the amount of energy that the Cisco IP Phone consumes by using Power Save or EnergyWise (Power Save Plus) mode.

Power Save

In Power Save mode, the backlight on the screen is not lit when the phone is not in use. The phone remains in Power Save mode for the scheduled duration or until the user lifts the handset or presses any button.

Set up each phone to enable or disable Power Save settings. You can configure the phones to dim the backlight on a schedule.

Power Save Plus (EnergyWise)

The Cisco IP Phone supports Cisco EnergyWise (Power Save Plus) mode. When your network contains an EnergyWise (EW) controller (for example, a Cisco switch with the EnergyWise feature enabled), you can configure these phones to sleep (power down) and wake (power up) on a schedule to further reduce power consumption.

Set up each phone to enable or disable the EnergyWise settings. If EnergyWise is enabled, configure a sleep and wake time, as well as other parameters. These parameters are sent to the phone as part of the phone configuration XML file.

Related Topics

Schedule Power Save Plus (EnergyWise) on Cisco IP Phone, on page 174
Schedule Power Save for Cisco IP Phone, on page 173

Power Negotiation Over LLDP

The phone and the switch negotiate the power that the phone consumes. Cisco IP Phone operates at multiple power settings, which lowers power consumption when less power is available.

After a phone reboots, the switch locks to one protocol (CDP or LLDP) for power negotiation. The switch locks to the first protocol (containing a power Threshold Limit Value [TLV]) that the phone transmits. If the system administrator disables that protocol on the phone, the phone cannot power up any accessories because the switch does not respond to power requests in the other protocol.

Cisco recommends that Power Negotiation always be enabled (default) when connecting to a switch that supports power negotiation.

If Power Negotiation is disabled, the switch may disconnect power to the phone. If the switch does not support power negotiation, disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power the accessories up to the maximum that the IEEE 802.3af-2003 standard allows.

Note When CDP and Power Negotiation are disabled, the phone can power the accessories up to 15.4W.

Network Protocols

Cisco IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco IP Phones 8811, 8841, 8851, and 8861 support.

Table 5: Supported Network Protocols on the Cisco IP Phone

Network protocol	Purpose	Usage notes
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	Cisco IP Phones 8851 and 8861 support Bluetooth 4.0.

Network protocol	Purpose	Usage notes
Bootstrap Protocol (BootP)	BootP enables a network device, such as the Cisco IP Phone, to discover certain startup information, such as the IP address.	—
Cisco Audio Session Tunnel (CAST)	The CAST protocol allows Cisco IP Phones and associated applications to discover and communicate with the remote IP Phones without requiring changes to the traditional signaling components, such as Cisco Unified Communications Manager (CM) and gateways.	The Cisco IP Phone uses CAST as an interface between CUVA and Cisco Unified Communications Manager using the Cisco IP Phone as a SIP proxy.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco IP Phones use CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and the phone to become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the “Dynamic Host Configuration Protocol” chapter and the “Cisco TFTP” chapter in the *Cisco Unified Communications Manager System Guide*. **Note** If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco IP Phones use HTTP for XML services and for troubleshooting purposes.

Network protocol	Purpose	Usage notes
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco IP Phones that support HTTPS choose the HTTPS URL.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, and EAP-TLS. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN.
IEEE 802.11n/802.11ac	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11n operates at the 2,4 GHz and 5 GHz band and 802.11ac operates at the 5 GHz band.	The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the Cisco IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The Cisco IP Phones support IPv6 addresses. For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Internet Protocol Version 6 (IPv6)" chapter.
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco IP Phone supports LLDP on the PC port.

Network protocol	Purpose	Usage notes
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard for voice products.	The Cisco IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the LLDP-MED and Cisco Discovery Protocol white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice, over data networks.	Cisco IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round-trip delay) on RTP streams.	RTCP is enabled by default
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.

Network protocol	Purpose	Usage notes
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP addresses the functions of signaling and session management within a packet telephony network. Signaling allows transportation of call information across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. Cisco IP Phones support the SIP protocol when the phones are operating in IPv6 address, IPv4 address, or dual-stack mode.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	Upon security implementation, Cisco IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network that the DHCP server can automatically identify. If you want a phone to use a TFTP server other than the one that the DHCP server specifies, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone. For more information, see the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP signaling on the phones do not support UDP.

Related Topics

802.1X Authentication, on page 139

Configure Network Settings, on page 51
Phone Startup Verification, on page 65
VLAN Interaction, on page 13
Cisco Unified Communications Manager Interaction, on page 13
Cisco Unified Communications Manager Express Interaction, on page 14
Set Up the Audio and Video Port Range

VLAN Interaction

The Cisco IP Phone contains an internal Ethernet switch, enabling forwarding of packets to the phone, and to the computer (access) port and the network port on the back of the phone.

If a computer is connected to the computer (access) port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices that connect to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port to which the phone connects would be configured for separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC that connects to the switch through the computer (access) port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network that does not have enough IP addresses for each phone.

For more information, see the documentation that is included with a Cisco switch. You can also access switch information at this URL:

http://cisco.com/en/US/products/hw/switches/index.html

Related Topics

Network Protocols, on page 8

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is an open, industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Certificate Trust List (CTL) and Identity Trust List (ITL) files using the TFTP service

- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP phones described in this chapter, see the "Cisco IP Phone Configuration" chapter in the *Cisco Communications Manager Administration Guide*.

Note If the Cisco IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, install the latest support patch for your version of Cisco Unified Communications Manager from Cisco.com.

Related Topics

Network Protocols, on page 8

Cisco Unified Communications Manager Express Interaction

When the Cisco IP Phone works with the Cisco Unified Communications Manager Express (Unified CME), the phones must go into CME mode.

When a user invokes the conference feature, the tag allows the phone to use either a local or network hardware conference bridge.

The Cisco IP Phones do not support the following actions:

- Transfer: Only supported in the connected call transfer scenario.
- Conference: Only supported in the connected call transfer scenario.
- Join: Supported using the Conference button or hookflash access.
- Hold: Supported using the Hold button.
- Barge: Not supported.
- Direct Transfer: Not supported.
- Select: Not supported.

The users cannot create conference and transfer calls across different lines.

Related Topics

Network Protocols, on page 8

Voice Messaging System Interaction

Cisco Unified Communications Manager lets you integrate with different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide the following information to each user:

- How to access the voice messaging system account.

  Make sure that you have used Cisco Unified Communications Manager to configure the Messages button on the Cisco IP Phone.

- Initial password for accessing the voice messaging system.

  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

Phone Startup Overview

When connecting to the VoIP network, the Cisco IP Phones goes through a standard startup process. Depending on your specific network configuration, only some of these steps may occur on your Cisco IP Phone.

1 Obtain power from the switch. If a phone is not using external power, the switch provides inline power through the Ethernet cable that is attached to the phone.

2 (For a Cisco IP Phone 8861 in a wireless LAN only) Scan for an access point. The Cisco IP Phone 8861 scans the RF coverage area with the radio. The phone searches the network profiles and scans for access points that contain a matching SSID and authentication type. The phone associates with the access point with the highest RSSI that matches with the network profile.

3 (For a Cisco IP Phone 8861 in a wireless LAN only) Authenticate with the access point. The Cisco IP Phone begins the authentication process. The following table describes the authentication process:

Authentication type	Key management options	Description
Open	None	Any device can authenticate to the access point. For added security, static WEP encryption might optionally be used.
Shared Key	None	The phone encrypts the challenge text by using the WEP key and the access point must verify the WEP key that was used to encrypt the challenge text before network access is available.
PEAP or EAP-FAST	None	The RADIUS server authenticates the username and password before network access is available.

4 Load the stored phone image. The Cisco IP At startup, the phone runs a bootstrap loader that loads a phone firmware image that is stored in flash memory. Using this image, the phone initializes the software and hardware.

5 Configure the VLAN. If the Cisco IP Phone is connected to a Cisco Catalyst switch, the switch next informs the phone of the voice VLAN that is defined on the switch. The phone needs to know the VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.

6 Obtain an IP address. If the Cisco IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.

7 Request the CTL file. The TFTP server stores the CTL file. This file contains the certificates that are necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.

For more information, see the *Cisco Unified Communications Manager Security Guide*, "Configuring the Cisco CTL Client" chapter.

8 Request the ITL file. The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature signed by the servers. Cisco Unified Communications Manager 8.5 and later supports the ITL file.

9 Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the Cisco IP Phone to a TFTP Server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly.

Note You can also assign an alternate TFTP server to use instead of the one that DHCP assigns.

10 Request the configuration file. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.

11 Contact Cisco Unified Communications Manager. The configuration file defines how the Cisco IP Phone communicates with Cisco Unified Communications Manager and provides a phone with the load ID. After it obtains the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list.

If the security profile of the phone is configured for secure signaling (encrypted or authenticated) and the Cisco Unified Communications Manager is set to secure mode, the phone makes a TLS connection. Otherwise, the phone makes a nonsecure TCP connection.

If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and autoregistration is enabled in Cisco Unified Communications Manager, the phone attempts to autoregister itself in the Cisco Unified Communications Manager database.

Note Autoregistration is disabled when you configure the CTL client. In this case, you must add the phone to the Cisco Unified Communications Manager database manually.

External Devices

We recommend using good-quality external devices, such as headsets, cables, and connectors, that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals.

Note Not all Cisco IP Telephony products support external devices, cords or cables. For more information, consult the documentation for your endpoint.

Depending on the quality of these devices and their proximity to other devices, such as mobile phones or two-way radios, some audio noise may still occur. In these cases, Cisco recommends that you take one or more of these actions:

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of external devices, cables, and connectors.

Caution In European Union countries, use only external speakers, microphones, and headsets that are fully compliant with the EMC Directive [89/336/EC].

USB Port Information

The Cisco IP Phones 8851 and 8861 support a maximum of five devices that connect to each USB port. Each device that connects to the phone is included in the maximum device count. For example, your phone can support five USB devices on the side port and five additional standard USB devices on the back port. Many third-party USB products count as multiple USB devices; for example, a device containing a USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Note

- Unpowered hubs are not supported, and powered hubs with more than four ports are not supported.
- USB headsets that connect to the phone through a USB hub are not supported.

Each Cisco IP Phone 8800 Key Expansion Module (KEM) connected to the phone counts as a USB device. If three KEMs are connected to the phone, these count as three USB devices.

Phone Configuration Files

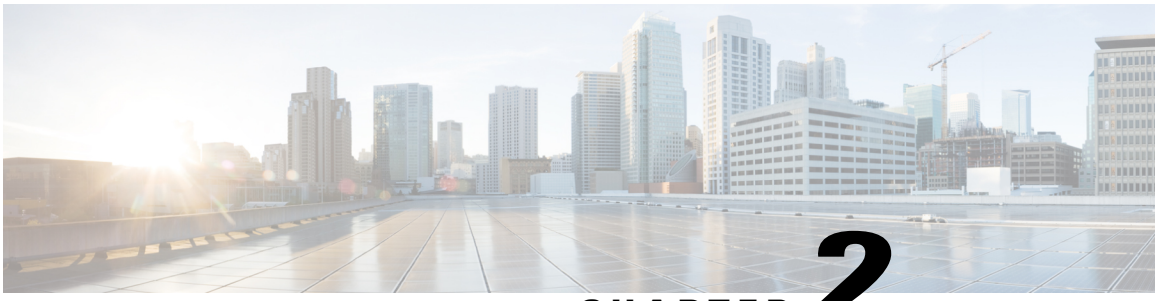
Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the phone configuration file.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

A phone accesses a default configuration file named XmlDefault.cnf.xml from the TFTP server when the following conditions exist:

- You have enabled autoregistration in Cisco Unified Communications Manager
- The phone has not been added to the Cisco Unified Communications Manager database
- The phone is registering for the first time



CHAPTER 2

Cisco IP Phone Hardware

- Phone Overview, page 19
- Cisco IP Phone 8811, page 20
- Cisco IP Phone 8841, page 25
- Cisco IP Phone 8851, page 29
- Cisco IP Phone 8861, page 33
- Terminology Differences, page 38

Phone Overview

The Cisco IP Phones 8811, 8841, 8851, and 8861 provides voice communication over an Internet Protocol (IP) network. The Cisco IP Phone functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phone connects to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizable features and services.

The Cisco IP Phone 8811 has a grayscale LCD screen.

The Cisco IP Phones 8841, 8851, and 8861 has a 24-bit color LCD screen.

The Cisco IP Phones have the following features:

- Programmable feature buttons that support up to 5 lines or that can be programmed for other features
- Gigabit ethernet connectivity
- Bluetooth support for wireless headsets(Cisco IP Phone 8851 and 8861 only)
- Support for an external microphone and speakers (Cisco IP Phone 8861 only)
- Network connectivity by Wi-Fi (Cisco IP Phone 8861 only)
- USB ports:
  - one USB port for Cisco IP Phone 8851
  - two USB ports for Cisco IP Phone 8861

A Cisco IP Phone, like other network devices, must be configured and managed. These phones encode and decode the following codes:

- G.711 a-law
- G.711 mu-law
- G.722
- G.729a/G.729ab
- G.726
- iLBC
- L16
- OPUS
- iSAC

Caution Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco IP Phone might cause interference. For more information, see the manufacturer's documentation of the interfering device.

Cisco IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco IP Phones also provide a variety of other features.

As with other network devices, you must configure Cisco IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone. If your network requires it, however, you can manually configure information such as: an IP address, TFTP server, and subnet information.

Cisco IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate Cisco Unified Communications Manager with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for coworker contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information.

Finally, because the Cisco IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. You can also obtain statistics about a current call or firmware versions on the phone.

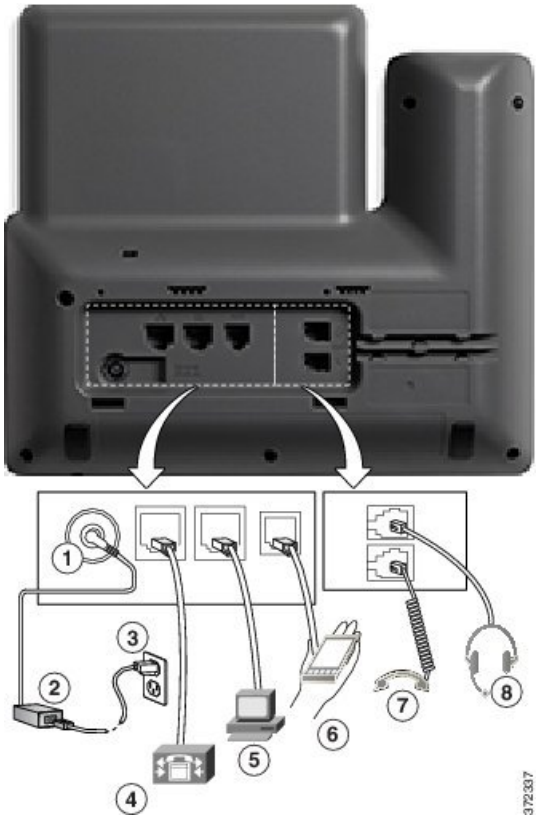
To function in the IP telephony network, the Cisco IP Phone must connect to a network device, such as a Cisco Catalyst switch. You must also register the Cisco IP Phone with a Cisco Unified Communications Manager system before sending and receiving calls.

Cisco IP Phone 8811

The following sections describe attributes of the Cisco IP Phone 8811.

Phone Connections

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adaptor port (DC48V).	5	Access port (10/100/1000 PC) connection.
2	AC-to-DC power supply (optional).	6	Auxiliary port.
3	AC power wall plug (optional).	7	Handset connection.
4	Network port (10/100/1000 SW) connection. IEEE 802.3at power enabled.	8	Analog headset connection (optional).

Note The Cisco IP Phone 8811 does not support the Cisco IP Phone 8800 Key Expansion Module.

Buttons and Hardware

1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings. The Cisco IP Phone 8811 screen is grayscale.

3	Programmable feature buttons and Session buttons	Your phone provides quick access to your phone lines, features, and call sessions: • Programmable feature buttons (left side): Use to view calls on a line or access features such as Speed Dial or All Calls. These buttons are also called feature buttons. • Session buttons (right side): Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button. **Note** If you are using a locale that reads right to left, such as Arabic, the line button and session button locations are swapped. Depending on how your system administrator sets up the phone, the buttons provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
4	Softkey buttons	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Navigation cluster and Select button	The Navigation cluster and Select button allows you to scroll through menus, highlight items, and select the highlighted item.
6	Release Button	Ends a connected call or session.

7	Hold/Resume button	Places an active call on hold and resumes the held call.
8	Conference button	Creates a conference call.
9	Transfer button	Transfers a call.
10	Speakerphone button	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Mute button	Toggles the microphone on or off. When the microphone is muted, the button is lit.
12	Headset button	Toggles the headset on or off. When the headset is on, the button is lit.
13	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
14	Volume button	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
15	Contacts button	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
16	Applications button	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.

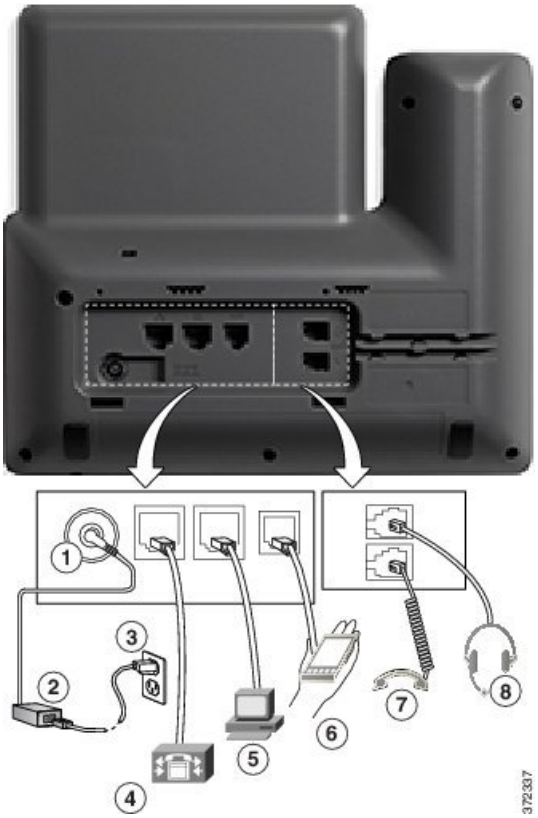
17	Messages button	Autodials your voice messaging system (varies by system).
18	Back button	Returns to the previous screen or menu.
19	Handset	Phone handset.

Cisco IP Phone 8841

The following sections describe attributes of the Cisco IP Phone 8841.

Phone Connections

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adaptor port (DC48V).	5	Access port (10/100/1000 PC) connection.
2	AC-to-DC power supply (optional).	6	Auxiliary port.
3	AC power wall plug (optional).	7	Handset connection.
4	Network port (10/100/1000 SW) connection. IEEE 802.3at power enabled.	8	Analog headset connection (optional).

Note The Cisco IP Phone 8841 does not support the Cisco IP Phone 8800 Key Expansion Module.

Buttons and Hardware

1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.

3	Programmable feature buttons and Session buttons	Your phone provides quick access to your phone lines, features, and call sessions: • Programmable feature buttons (left side): Use to view calls on a line or access features such as Speed Dial or All Calls. These buttons are also called feature buttons. • Session buttons (right side): Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button. **Note** If you are using a locale that reads right to left, such as Arabic, the line button and session button locations are swapped. Depending on how your system administrator sets up the phone, the buttons provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
4	Softkey buttons	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Navigation cluster and Select button	The Navigation cluster and Select button allows you to scroll through menus, highlight items and select the highlighted item.
6	Release Button	Ends a connected call or session.

7	Hold/Resume button	Places an active call on hold and resumes the held call.
8	Conference button	Creates a conference call.
9	Transfer button	Transfers a call.
10	Speakerphone button	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Mute button	Toggles the microphone on or off. When the microphone is muted, the button is lit.
12	Headset button	Toggles the headset on or off. When the headset is on, the button is lit.
13	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
14	Volume button	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
15	Contacts button	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
16	Applications button	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.

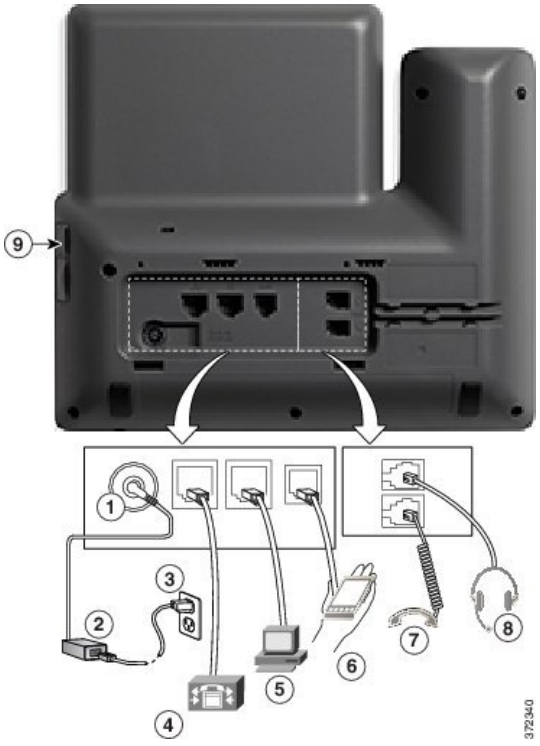
17	Messages button	Autodials your voice messaging system (varies by system).
18	Back button	Returns to the previous screen or menu.
19	Handset	Phone handset.

Cisco IP Phone 8851

The following sections describe attributes of the Cisco IP Phone 8851.

Phone Connections

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adaptor port (DC48V).	5	Access port (10/100/1000 PC) connection.	9	USB port
2	AC-to-DC power supply (optional).	6	Auxiliary port.		
3	AC power wall plug (optional).	7	Handset connection.		
4	Network port (10/100/1000 SW) connection. IEEE 802.3at power enabled.	8	Analog headset connection (optional).		

Note Each USB port supports the connection of up to five supported and nonsupported devices. Each device connected to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as two Cisco IP Phone 8800 Key Expansion Modules, one headset, one hub, and one other standard USB device) on the side port. Many third-party USB products count as multiple USB devices, for example, a device containing USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Buttons and Hardware

1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).

2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.
3	Programmable feature buttons and Session buttons	Your phone provides quick access to your phone lines, features, and call sessions: • Programmable feature buttons (left side): Use to view calls on a line or access features such as Speed Dial or All Calls. These buttons are also called feature buttons. • Session buttons (right side): Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button. **Note** If you are using a locale that reads right to left, such as Arabic, the line button and session button locations are swapped. Depending on how your system administrator sets up the phone, the buttons provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
4	Softkey buttons	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Navigation cluster and Select button	The Navigation cluster and Select button allows you to scroll through menus, highlight items and select the highlighted item.

6	Release Button	Ends a connected call or session.
7	Hold/Resume button	Places an active call on hold and resumes the held call.
8	Conference button	Creates a conference call.
9	Transfer button	Transfers a call.
10	Speakerphone button	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Mute button	Toggles the microphone on or off. When the microphone is muted, the button is lit.
12	Headset button	Toggles the headset on or off. When the headset is on, the button is lit.
13	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
14	Volume button	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
15	Contacts button	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.

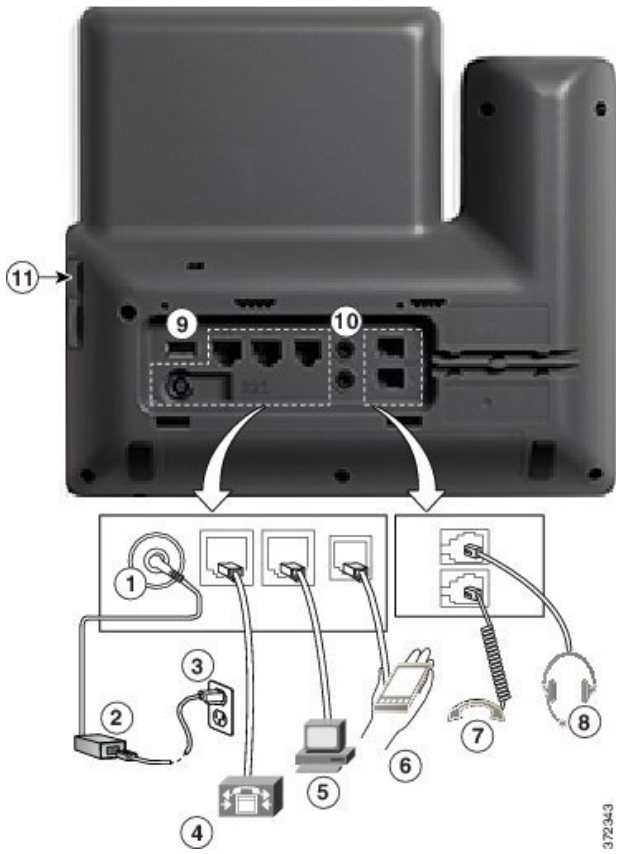
16	Applications button	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
17	Messages button	Autodials your voice messaging system (varies by system).
18	Back button	Returns to the previous screen or menu.
19	Handset	Phone handset.

Cisco IP Phone 8861

The following sections describe attributes of the Cisco IP Phone 8861.

Phone Connections

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adaptor port (DC48V).	6	Auxiliary port.	11	USB port
2	AC-to-DC power supply (optional).	7	Handset connection.		
3	AC power wall plug (optional).	8	Analog headset connection (optional).		
4	Network port (10/100/1000 SW) connection. IEEE 802.3at power enabled.	9	USB port		
5	Access port (10/100/1000 PC) connection.	10	Audio In/Out ports		

Note Each USB port supports the connection of up to five supported and nonsupported devices. Each device connected to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as three Cisco IP Phone 8800 Key Expansion Modules, one hub, and one other standard USB device) on the side port and five additional standard USB devices on the back port. Many third-party USB products count as multiple USB devices, for example, a device containing USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Buttons and Hardware

1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.

3	Programmable feature buttons and Session buttons	Your phone provides quick access to your phone lines, features, and call sessions: • Programmable feature buttons (left side): Use to view calls on a line or access features such as Speed Dial or All Calls. These buttons are also called feature buttons. • Session buttons (right side): Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button. **Note** If you are using a locale that reads right to left, such as Arabic, the line button and session button locations are swapped. Depending on how your system administrator sets up the phone, the buttons provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
4	Softkey buttons	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Navigation cluster and Select button	The Navigation cluster and Select button allows you to scroll through menus, highlight items and select the highlighted item.
6	Release Button	Ends a connected call or session.

7	Hold/Resume button	Places an active call on hold and resumes the held call.
8	Conference button	Creates a conference call.
9	Transfer button	Transfers a call.
10	Speakerphone button	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Mute button	Toggles the microphone on or off. When the microphone is muted, the button is lit.
12	Headset button	Toggles the headset on or off. When the headset is on, the button is lit.
13	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
14	Volume button	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
15	Contacts button	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
16	Applications button	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.

17	Messages button	Autodials your voice messaging system (varies by system).
18	Back button	Returns to the previous screen or menu.
19	Handset	Phone handset.

Terminology Differences

The following table highlights some of the differences in terminology found in the *Cisco IP Phone 8811, 8841, 8851, and 8861 User Guide for Cisco Unified Communications Manager* , the *Cisco IP Phone 8811, 8841, 8851, and 8861 Administration Guide for Cisco Unified Communications Manager*, and the *Cisco Unified Communications Manager Administration Guide*.

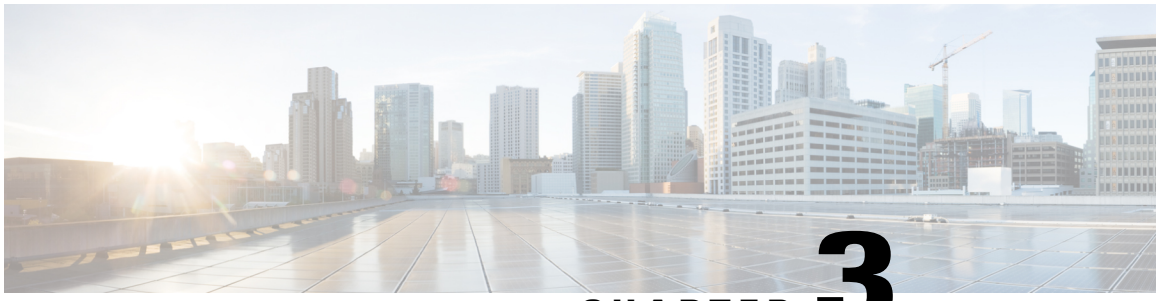
Table 6: Terminology Differences

User Guide	Administration Guide
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Programmable Feature Button	Programmable Button or Programmable Line Key (PLK)
Simplified New Call Window	Simplified New Call Bubble
Voicemail System	Voice Messaging System

PART II

Cisco IP Phone Installation

- Cisco IP Phone Installation, page 41
- Cisco Unified Communications Manager Phone Setup, page 67
- Self Care Portal Management, page 79



CHAPTER 3

Cisco IP Phone Installation

- Verify Network Setup, page 41
- Enable Autoregistration for Phone, page 42
- Install Cisco IP Phone, page 43
- Set Up Phone from Setup Menus, page 44
- Set Up Wireless LAN, page 46
- Configure Network Settings, page 51
- Phone Startup Verification, page 65
- Configure Phone Services for Users, page 65

Verify Network Setup

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a Cisco IP telephony network, see the "System Configuration Overview" chapter in *Cisco Unified Communications Manager System Guide*.

For the phone to successfully operate as an endpoint in your network, your network must meet specific requirements.

Note The phone displays the date and time from Cisco Unified Communications Manager. The time displayed on the phone can differ from the Cisco Unified Communications Manager time by up to 10 seconds.

Procedure

Step 1 Configure a VoIP Network to meet the following requirements:

- VoIP is configured on your Cisco routers and gateways.

- Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.

Step 2 Set up the network to support one of the following:

- DHCP support
- Manual assignment of IP address, gateway, and subnet mask

Enable Autoregistration for Phone

The Cisco IP Phone requires Cisco Unified Communications Manager to handle call processing. See the *Cisco Unified Communications Manager Administration Guide* or the context-sensitive help in the Cisco Unified Communications Manager Administration to ensure that Cisco Unified Communications Manager is set up properly to manage the phone and to properly route and process calls.

Before you install the Cisco IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database.

By enabling autoregistration before you install the phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move autoregistered phones to new locations and assign them to different device pools without affecting their directory numbers.

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone, or if you want to use a secure connection with Cisco Unified Communications Manager as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling autoregistration, see the "Enabling Autoregistration" section in the *Cisco Unified Communications Manager Administration Guide*. When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

You can add phones with autoregistration and TAPS, the Tool for AutoRegistered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and to download predefined configurations for phones.

Cisco recommends that you use autoregistration and TAPS to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

To implement TAPS, you or the end user dials a TAPS directory number and follows voice prompts. After the process is complete, the phone contains the directory number and other settings, and the phone is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Verify that autoregistration is enabled and is properly configured in Cisco Unified Communications Manager Administration before you connect any Cisco IP Phone to the network. For information about enabling and configuring autoregistration, see the *Cisco Unified Communications Manager Administration Guide*.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration for TAPS to function.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **System** > **Cisco Unified CM**.

Step 2 Select the required server and then select the Autoregister check box.

Step 3 In **Auto-registration Information**, configure Universal Device Template, Universal Line Template, Starting Directory Number, and Ending Directory Number.

Step 4 Click **Save**.

Related Topics

Phone Addition Methods, on page 71

Install Cisco IP Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable DHCP service.

If you used autoregistration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

Note Before using external devices, read External Devices, on page 16.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

For more information, see Phone Power Requirements, on page 6.

Step 2 Connect the handset to the handset port.
The wideband-capable handset is designed especially for use with a Cisco IP Phone. The handset includes a light strip that indicates incoming calls and waiting voice messages.

Step 3 Connect a headset or wireless headset. You can add a headset later if you do not connect one now. For more information, see Headsets, on page 85 or Wireless Headsets, on page 89.

Step 4 Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100/1000 SW on the Cisco IP Phone. Each Cisco IP Phone ships with one Ethernet cable in the box. Use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts, on page 4.

Step 5 Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the Cisco IP Phone. You can connect another network device later if you do not connect one now.
You can use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts, on page 4 for guidelines.

Step 6 If the phone is on a desk, adjust the footstand. For more information, see Connect Footstand, on page 84.
With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle. For more information, seeAdjust the Handset Rest, on page 122

Step 7 Monitor the phone startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the phone, and verifies that the phone is configured properly.

Step 8 If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.
See Configure Network Settings, on page 51 and Network Setup, on page 231.

Step 9 Upgrade the phone to the current firmware image.
Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than one hour.

Step 10 Make calls with the Cisco IP Phone to verify that the phone and features work correctly.
See the *Cisco IP Phone 8811, 8841, 8851, and 8861 User Guide for Cisco Unified Communications Manager*.

Step 11 Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco IP Phones.

Set Up Phone from Setup Menus

The Cisco IP Phone includes the following configuration menus:

- Network Setup: Provides options for viewing and configuring network settings such as IPv4, IPv6, WLAN, and Ethernet.
  - Ethernet Setup: The menu items in this submenu provide configuration options to configure the Cisco IP Phone over an ethernet network.
  - WiFi Client Setup: The menu items in this submenu provide configuration options to configure the Cisco IP Phone with the wireless local area network (WLAN).
  - IPv4 Setup and IPv6 Setup: These submenus of the Ethernet Setup menu and of the WiFi Client Setup menu provide additional network options.

- Security Setup: Provides options for viewing and configuring security settings such as security mode, the trust list and 802.1X authentication.

Before you can change option settings on the Network Setup menu, you must unlock options for editing.

Note You can control whether a phone has access to the Settings menu or to options on this menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. The Settings Access field accepts these values:

- Enabled: Allows access to the Settings menu.
- Disabled: Prevents access to the Settings menu.
- Restricted: Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Administrator Settings menu, check the Settings Access field.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings**.

Step 3 Select **Network Setup** or **Security Setup**.

Step 4 Enter your user ID and password, if required, and click **Sign-In**.

Step 5 Perform one of these actions to display the desired menu:

- Use the navigation arrows to select the desired menu and then press **Select**.
- Use the keypad on the phone to enter the number that corresponds to the menu.

Step 6 To display a submenu, repeat step 5.

Step 7 To exit a menu, press **Exit** or the back arrow.

Apply Phone Password

You can apply a password to the phone so that no changes can be made to the administrative options on the phone without password entry on the Administrator Settings phone screen.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window using **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Enter a password in the Local Phone Unlock Password option.

Step 3 Apply the password to the common phone profile that the phone uses.

Text Menu Entry from Phone

When you edit the value of an option setting, follow these guidelines:

- Use the arrows on the navigation pad to highlight the field that you wish to edit, then press **Select** in the navigation pad to activate the field. After the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
- Press the arrow softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Cancel** before pressing **Save** to discard any changes that you made.
- To enter an IP address, you enter values into four segments already divided for you. When you have finished entering the leftmost digits before the first period, use the right arrow key to move to the next segment. The period that follows the leftmost digits is automatically inserted.
- To enter a colon for an IPv6 address, press * on the keypad.

Note The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

Related Topics

Basic Reset, on page 263
Apply Phone Password, on page 45

Set Up Wireless LAN

Ensure that the Wi-Fi coverage in the location where the wireless LAN is deployed is suitable for transmitting voice packets.

If the Wi-Fi connectivity for voice is enabled for the Cisco IP Phone and you are using EAP-FAST or PEAP security mode, you authenticate the Wi-Fi network by using the WLAN Sign in application within your applications menu. WEP, PSK, and open security modes authenticate on the Wi-Fi network.

For complete configuration information, see the *Cisco IP Phone 8800 Wireless LAN Deployment Guide* at this location:

http://www-author.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html

The *Cisco IP Phone 8800 Wireless LAN Deployment Guide* includes the following configuration information:

- Wireless network configuration
- Wireless network configuration in Cisco Unified Communications Manager Administration
- Wireless network configuration on the Cisco IP Phone

Procedure

Step 1 To enable the application, go to **Applications** > **Administrator Settings** > **Network Setup** > **Wi-Fi Client Setup** > **Wi-Fi Sign in Access**.

Step 2 Enable Wireless network.

Step 3 To change the username or password, go to **Applications** > **Administrator Settings**.

Set Up Wireless LAN from Cisco Unified Communications Manager

In Cisco Unified Communications Manager Administration, you must enable a parameter called “Wi-Fi” for the wireless Cisco IP Phone.

Note In the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Phone**), use the wired-line MAC address when you configure the MAC address. Cisco Unified Communications Manager registration does not use the wireless MAC address.

Perform the following procedure in Cisco Unified Communications Manager Administration.

Procedure

Step 1 To enable the wireless LAN on a specific phone perform the following steps:

a) Select **Device** > **Phone**.
b) Locate the required phone.
c) Select the enable setting for the Wi-Fi parameter in the Product Specific Configuration Layout section
d) Check the Override Common Settings check box

Step 2 To enable wireless LAN for a group of phones,

a) Select **Device** > **Device Settings** > **Common Phone Profile**.
b) Select the enable setting for the Wi-Fi parameter
c) Check the Override Common Settings check box

d) Associate the phones with that common phone profile using **Device** > **Phone** .

Step 3 To enable wireless LAN for all WLAN-capable phones in your network,

a) Select **System** > **Enterprise Phone Configuration**.
b) Select the enable setting for the Wi-Fi parameter.
c) Check the Override Common Settings check box.

Set Up Wireless LAN from Phone

Before the Cisco IP Phone can connect to the WLAN, you must configure the network profile for the phone with the appropriate WLAN settings. You can use the Network Setup menu on the phone to access the WiFi Client Setup submenu and set up the WLAN configuration.

Note You can configure the Wireless settings only on the Cisco IP Phone keypad. You must use the AC adapter when you use the Cisco IP Phone in Wireless mode. Wireless is disabled when Ethernet is connected.

Note The WiFi Client Setup option does not appear in the Network Setup menu when WiFi is disabled on the Cisco Unified Communications Manager.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **Wi-Fi Client Setup**.

Step 3 Set up the wireless configuration as described in the following table.

Table 7: WiFi Client Setup Menu Options

Option	Description	To change
Wireless	Turns the wireless radio on Cisco IP Phone on or off. Valid values specify: • On: Turns the wireless radio on the phone on. • Off: Turns the wireless radio on the phone off. Default: On	See Set Wireless Field, on page 61.

Option	Description	To change
Wireless Sign in Access	Enables the display of the Wireless Sign in Access window in the main Applications menu: • On: The Wireless Sign In Access window displays. Turning this value on allows you to sign in or change your Wireless user ID and password on the main Applications menu. Otherwise, to change your sign-in information, navigate down to the Security menu level and select either the PEAP or EAP-FAST methods, both of which require sign-in credentials. • Off: The Wireless Sign In Access window does not display. Default: Off	See Set WLAN Sign In Access Field, on page 61.
IPv4 Setup	In the IPv4 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IP address that the DHCP server assigns. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. For more information about the IPv4 address fields, see Set Up IPv4, on page 54.	Scroll to IPv4 Setup and press **Select**.
IPv6 Setup	In the IPv6 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IPv6 address that is either assigned by DHCPv6 server or acquired by SLAAC through an IPv6-enabled router. • Manually set the IPv6 Address, Prefix Length, Default Routers, DNS Server, and Alternate TFTP servers. For more information about the IPv6 address fields, see Set Up IPv6, on page 57.	Scroll to IPv6 Setup and press **Select**.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only. Cannot configure.

Option	Description	To change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Set Domain Name Field, on page 60.
SSID	Specifies the Service Set Identifier, a unique identifier for accessing wireless access points.	See Set SSID Field, on page 61.
Security Mode	The type of authentication that the phone uses to access the WLAN. Valid values specify: • None: Access to all access points (APs) without encryption. • WEP: Open 802.11 authentication but uses Wired Equivalent Privacy (WEP) for encrypting the data. Specifies access to all APs and authentication through WEP keys at the local AP. • PSK: Shared key authentication using WEP. • EAP-FAST: Extensible Authentication Protocol Flexible Authentication via Secure Tunneling exchanges a username and cryptographically secure password with a RADIUS server in the network where a PAC (Protected Access Credential) establishes a secure tunnel for authentication. EAP-FAST supports WPA and WPA2. • PEAP(MSCHAPV2): Protected Extensible Authentication Protocol authentication exchanges a username and cryptographically secure password with a RADIUS server in the network. PEAP is a Cisco proprietary version of EAP. PEAP supports WPA and WPA2.	See Set Security Mode Field, on page 62.
802.11 Mode	Specifies the wireless signal standard that is used in the WLAN. Valid values specify: • Auto: Default value. • 2.4 Ghz • 5.0 Ghz	See Set 802.11 Mode Field, on page 62 .

Configure Network Settings

If you are not using DHCP in your network, you must configure these network settings on the Cisco IP Phone after you install the phone on the network:

- IP address
- IP subnet information
- IPv6 addresses
- TFTP server IP address

If necessary, you may also configure the domain name and the DNS server settings.

The Ethernet Setup menu provides options for viewing and changing a variety of network settings. The following table describes these options and, where applicable, explains how to change them.

Note Establishing a VPN connection overwrites the Ethernet data fields.

Table 8: Ethernet Setup Menu Options

Option	Description	To change
IPv4 Setup	In the IPv4 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IP address that the DHCP server assigns. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. This option displays only when the phone is configured in IPv4-only mode or in dual-stack mode.	Scroll to IPv4 Setup and press **Select**. See Set Up IPv4, on page 54.
IPv6 Setup	The IPv6 configuration for the phone.	Scroll to IPv6 Setup and press **Select** See Set Up IPv6, on page 57.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only. Cannot configure.

Option	Description	To change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Set Domain Name Field, on page 60.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch of which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	Display only. Cannot configure. The phone obtains the Operational VLAN ID via Cisco Discovery Protocol (CDP) or Link Level Discovery Protocol Media Endpoint Discovery (LLDP-MED). This information comes from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin VLAN ID	Auxiliary VLAN of which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise, this value is ignored.	See Set Admin VLAN ID Field, on page 60.
PC VLAN	Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	See Set PC VLAN Field, on page 60.

Option	Description	To change
SW Port Setup	Speed and duplex of the network port. Valid values specify: • Auto Negotiate • 1000 Full:1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	See Set SW Port Setup Field, on page 60.
PC Port Setup	Speed and duplex of the Computer (access) port. Valid values: • Auto Negotiate • 1000 Full: 1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	See Set PC Port Setup Field, on page 61. To configure the setting on multiple phones simultaneously, enable Remote Port Configuration in the Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**). **Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager Administration, the data cannot be changed on the phone.

Procedure

Step 1 Press **Applications** .

Step 2 To access the Network Settings menu, select **Administrator Settings** > **Network Setup**

Set Up IPv4

The following table describes the IPv4 Setup menu options.

Table 9: IPv4 Setup Menu Options

Option	Description	To change
DHCP Enabled	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone. For more information, see Set Up Phone to Use DHCP, on page 64 and Set Up Phone to Not Use DHCP, on page 65.	See Set DHCP Enabled Field, on page 62.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	See Set IP Address Field, on page 62.
Subnet Mask	Subnet mask used by the phone.	See Set Subnet Mask Field, on page 63.
Default Router	Default router used by the phone.	See Set Default Router Field, on page 63.
DNS Server 1 DNS Server 2 DNS Server 3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2 and 3) that the phone uses.	See Set DNS Server Fields, on page 63.
Alternate TFTP	Indicates whether the phone is using an alternate TFTP server.	See Set Alternate TFTP Field, on page 63.

Option	Description	To change
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to On, you must enter a nonzero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 1 option. In this case, the phone deletes the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file downloads from the new TFTP Server 1 address. When the phone looks for the TFTP server, the phone gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in this order: **1** Any manually assigned IPv4 TFTP servers **2** Any manually assigned IPv6 servers **3** DHCP assigned TFTP servers **4** DHCPv6 assigned TFTP servers **Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.	See Set TFTP Server 1 Field, on page 64.

Option	Description	To change
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address. When the phone looks for the TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in the following order: **1** Any manually assigned IPv4 TFTP servers **2** Any manually assigned IPv6 servers **3** DHCP assigned TFTP servers **4** DHCPv6 assigned TFTP servers **Note** For information about the CTL or ITL file, see Cisco Unified Communications Manager Security Guide.	See Set TFTP Server 2 Field, on page 64. If you forget to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing Erase from the Security Configuration menu. A new CTL or ITL file downloads from the new TFTP Server 2 address.
BOOTP Server	Indicates whether the phone received the IP address from a BOOTP server rather than from a DHCP server.	Display only.
DHCP Address Released	Releases the IP address that DHCP assigned.	This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this option to Yes and press Apply.

Procedure

Step 1 Press **Applications** .

Step 2 To access the Network Settings menu, select **Administrator Settings** > **Network Setup**

Step 3 To access the IPv4 settings menu, navigate to the IPv4 options from **Ethernet Setup** > **IPv4 Setup**.

Set Up IPv6

IPv6 addressing is supported on the phone. A valid IPv6 address is 128 bits in length, including the subnet prefix.

IPv6 addresses must be in one of the following formats:

- Eight sets of four hexadecimal digits separated by colons where the leftmost digits represent the highest-order bits. Any leading or trailing zeros in each group may be omitted.
- Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon. Note that this can only be done once in an address.

Before IPv6 setup options can be configured on your device, IPv6 must be enabled and configured in Cisco Unified Communication Administration. The following device configuration fields apply to IPv6 configuration:

- IP Addressing Mode
- IP Addressing Mode Preference for Signalling

If IPv6 is enabled in the Unified cluster, the default setting for IP addressing mode is IPv4 and IPv6 (dual-stack). In this addressing mode, the phone will acquire and use one IPv4 address and one IPv6 address. It can use the IPv4 and the IPv6 address as required for media. The phone uses either the IPv4 or IPv6 address for call control signalling to Unified CM.

For more information, see the section on Common Device Configuration in *Cisco Unified Communications Manager Feature and Services Guide*, "IPv6 Support in Cisco Unified Communications Devices".

Note Cisco recommends IPv4 and IPv6 as the setting for the phone addressing mode. IPv6 Only is not recommended for production environments.

You set up IPv6 from one of the following menus:

- When WiFi is disabled: **Ethernet Setup** > **IPv6 Setup**
- When WiFi is enabled: **Wi-Fi Client Setup** > **IPv6 Setup**

The following table describes the IPv6 related information found in the IPv6 menu.

Table 10: IPv6 Setup Menu Options

Option	Default value	Description
DHCPv6 Enabled	Yes	Indicates the method that the phone uses to get the IPv6 address. When DHCPv6 is enabled, the phone gets the IPv6 address either from DHCPv6 server or from SLAAC by RA sent by the IPv6-enabled router. And if DHCPv6 is disabled, the phone will not have any stateful (from DHCPv6 server) or stateless (from SLAAC) IPv6 address. **Note** Unlike DHCPv4, even DHCPv6 is disabled the phone can still generate a SLAAC address if autoconfigure is enabled.
IPv6 Address	::	Displays the current IPv6 address of the phone or allows the user to enter a new IPv6 address. Two address formats are supported: • Eight sets of hexadecimal digits separated by colons X:X:X:X:X:X:X:X • Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon. If the IP address is assigned with this option, you must also assign the IPv6 prefix length and the default router.
IPv6 Prefix Length	0	Displays the current prefix length for the subnet or allows the user to enter a new prefix length. The subnet prefix length is a decimal value from 1-128.
IPv6 Default Router	::	Displays the default router used by the phone or allows the user to enter a new IPv6 default router.
IPv6 DNS Server 1	::	Displays the primary DNSv6 server used by the phone or allows the user to enter a new server.
IPv6 DNS Server 2	::	Displays the secondary DNSv6 server used by the phone or allows the user to set a new secondary DNSv6 server.
IPv6 Alternate TFTP	No	Allows the user to enable the use of an alternate (secondary) IPv6 TFTP server.
IPv6 TFTP Server 1	::	Displays the primary IPv6 TFTP server used by the phone or allows the user to set a new primary TFTP server.
IPv6 TFTP Server 2	::	(Optional) Displays the secondary IPv6 TFTP server used if the primary IPv6 TFTP server is unavailable or allows the user to set a new secondary TFTP server.

Option	Default value	Description
IPv6 Address Released	No	Allows the user to release IPv6-related information.

Procedure

Step 1 Press **Applications** .

Step 2 To access the Network Settings menu, select **Administrator Settings** > **Network Setup**

Step 3 To access the IPv6 settings menu, perform one of the following actions:

- With Wi-Fi disabled on the Cisco Unified Communications Manager: navigate to **Ethernet Setup** > **IPv6 Setup**.
- With Wi-Fi enabled on the Cisco Unified Communications Manager: navigate to **Wi-Fi client Setup** > **IPv6 Setup**.

Step 4 To enter IPv6 addresses,

a) Click in an input field.

b) Make your changes to the field (see the information below).

The following table describes the address formats.

Format	Description
X:X:X:X:X:X:X:X	Eight sets of hexadecimal digits separated by colons. Leading or trailing zeros in each group may be omitted. Example: 2001:db8:0:0:0:52:0:1
Compressed	Collapse a single run of consecutive zero groups into a single group represented by a double colon. Example: 2001:db8::52:0:1

- To enter a colon (:) in the address, press the asterisk (*) on the keypad.
- To enter hexadecimal digits a, b, and c, press 2 on the keypad, scroll to select the required digit, and press **Enter**.
- To enter hexadecimal digits d, e, and f, press 3 on the keypad, scroll to select the required digit, and press **Enter**.
- After you enter each part of the address, you press **Apply** or **Revert** .

Step 5 Change toggle fields using these steps:

a) If an option is set to No, press **Yes** to enable it. If the option is set to Yes, press **No** to disable it.

b) Press **Apply** to save your change, or **Revert** to discard it.

Set Domain Name Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Domain Name option, press **Select**, and enter a new domain name.
Step 3 Press **Apply**.

Set Admin VLAN ID Field

Procedure

Step 1 Scroll to the Admin. VLAN ID option, press **Select**, and enter a new Admin VLAN ID setting.
Step 2 Press **Apply**.

Set PC VLAN Field

Procedure

Step 1 Ensure that the Admin VLAN ID option is set.
Step 2 Scroll to the PC VLAN option, press **Select**, and then enter a new PC VLAN setting.
Step 3 Press **Apply**.

Set SW Port Setup Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the SW Port Setup option and press **Select**.
Step 3 Scroll to the setting that you want and press **Select**.

Set PC Port Setup Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the PC Port Setup option and press **Select**.
Step 3 Scroll to the setting that you want and press **Select**.

Set Wireless Field

Procedure

Step 1 Scroll to the Wireless option, and use the toggle switch to change the setting between on and off.
Step 2 Press **Apply**.

Set WLAN Sign In Access Field

Procedure

Step 1 Scroll to the Wireless Sign In option, and use the toggle switch to change the setting between on and off.
Step 2 Press **Apply**.

Set SSID Field

Procedure

Step 1 Scroll to the SSID option, press **Select**, and enter an SSID.
Step 2 Press **Apply**.

Set Security Mode Field

Procedure

Step 1 Scroll to the Security Mode option, and highlight the desired value.
Step 2 Click **Apply**.

Set 802.11 Mode Field

Procedure

Step 1 Scroll to the 802.11 Mode option, and highlight the desired value.
Step 2 Click **Apply**.

Set DHCP Enabled Field

Procedure

Step 1 Scroll to the DHCP Enabled option.
Step 2 Press **No** to disable DHCP, or press **Yes** to enable DHCP.

Set IP Address Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the IP Address option, press **Select**, and enter a new IP Address.
Step 3 Press **Apply**.

Set Subnet Mask Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Subnet Mask option, press **Select**, and enter a new subnet mask.
Step 3 Press **Apply**.

Set Default Router Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate Default Router option, press **Select**, and enter a new router IP address.
Step 3 Press **Apply**.

Set DNS Server Fields

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate DNS Server option, press **Select**, and enter a new DNS server IP address.
Step 3 Press **Apply**.
Step 4 If multiple DNS Servers can be configured, repeat Steps 2 and 3 as needed to assign backup DNS servers.

Set Alternate TFTP Field

Procedure

Step 1 Scroll to the Alternate TFTP option.
Step 2 Press **Yes** if the phone should use an alternative TFTP server.
Step 3 Press **No** if the phone should not use an alternative TFTP server.

Set TFTP Server 1 Field

Procedure

Step 1 Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If the CTL and ITL files both exist, unlock either file.

Step 2 If DHCP is enabled, set the Alternate TFTP option to **Yes**.

Step 3 Scroll to the TFTP Server 1 option, press **Select**, and enter a new TFTP server IP address.

Step 4 Press **Apply** then press **Save**.

Set TFTP Server 2 Field

Procedure

Step 1 Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If both the CTL and ITL files exist, unlock either of the files.

Step 2 Unlock network configuration options.

Step 3 Enter an IP address for the TFTP Server 1 option.

Step 4 Scroll to the TFTP Server 2 option, press **Select**, and enter a new backup TFTP server IP address. If there is no secondary TFTP Server, you can use **Delete** to clear the field of a previous value.

Step 5 Press **Apply** and then press **Save**.

Set Up Phone to Use DHCP

To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco IP Phone and direct the phone to a TFTP server, perform these steps:

Procedure

Step 1 Press **Applications** and choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 2 To enable DHCP, set DHCP Enabled to **Yes**. DHCP is enabled by default.

Step 3 To use an alternate TFTP server, set Alternate TFTP Server to **Yes**, and enter the IP address for the TFTP Server.

Note Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server that DHCP assigns.

Step 4 Press **Apply**,

Set Up Phone to Not Use DHCP

When not using DHCP, you must configure the IP address, subnet mask, TFTP server, and default router locally on the phone.

Procedure

Step 1 Press **Applications** and choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 2 To disable DHCP and manually set an IP address:

a) Set DHCP Enabled to **No**.
b) Enter the static IP address for phone.
c) Enter the subnet mask.
d) Enter the default router IP addresses.
e) Set Alternate TFTP Server to **Yes**, and enter the IP address for TFTP Server 1.

Step 3 Press **Apply**.

Phone Startup Verification

After the Cisco IP Phone has power connected to it, the phone begins the startup diagnostic process by cycling through the following steps.

1. The Feature and Session buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.
2. The main screen displays `Registering to Cisco Unified Communications Manager`.

If the phone completes these stages successfully, it has started up properly and the **Select** button stays lit until it is selected.

Related Topics

Startup Problems, on page 247
Cisco IP Phone Does Not Go Through Normal Startup Process, on page 247
Network Protocols, on page 8

Configure Phone Services for Users

You can give users access to Cisco IP Phone Services on the IP phone. You can also assign a button to different phone services. These services comprise XML applications and Cisco-signed Java midlets that enable the display of interactive content with text and graphics on the phone. The IP phone manages each service as a separate application. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

- You must use Cisco Unified Communications Manager Administration to configure services that are not present by default.

- The user must subscribe to services by using the Cisco Unified Communications Self Care Portal. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP phone applications. However, a user cannot subscribe to any service that you configure as an enterprise subscription.

For more information, see the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications ManagerAdministration Guide* and the "Cisco Unified IP Phone Services" chapter in the *Cisco Unified Communications Manager System Guide*.

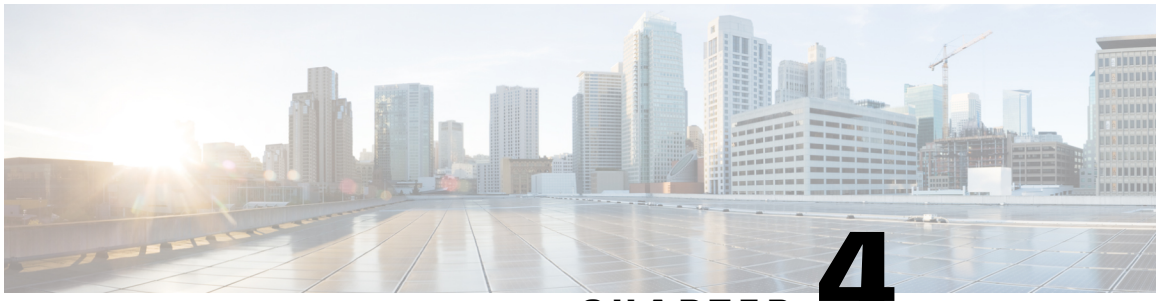
Note To configure Cisco Extension Mobility services for users, see the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Before you set up services, gather the URLs for the sites that you want to set up and verify that users can access those sites from your corporate IP telephony network. This activity is not applicable for the default services that Cisco provides.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**

Step 2 Verify that your users can access the Cisco Unified Communications Self Care Portal, from which they can select and subscribe to configured services.
See Self Care Portal Management, on page 79 for a summary of the information that you must provide to end users.



CHAPTER 4

Cisco Unified Communications Manager Phone Setup

- Set Up Cisco IP Phone, page 67
- Determine Phone MAC Address, page 70
- Phone Addition Methods, page 71
- Add Users to Cisco Unified Communications Manager, page 72
- Add User to End User Group, page 74
- Associate Phones with Users , page 74
- Survivable Remote Site Telephony, page 75
- Set Up Cisco Unified Communications Manager Features, page 77

Set Up Cisco IP Phone

If autoregistration is not enabled and the phone does not exist in the Cisco Unified Communications Manager database, you must configure the Cisco IP Phone in Cisco Unified Communications Manager manually. Some tasks in this procedure are optional, depending on your system and user needs.

For more information about Cisco Unified Communications Manager Administration, see the *Cisco Unified Communications Manager Administration Guide*.

Perform the configuration steps in the following procedure using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Gather the following information about the phone:

- Phone model
- MAC address
- Physical location of the phone

- Name or user ID of phone user
- Device pool
- Partition, calling search space, and location information
- Number of lines and associated directory numbers (DNs) to assign to the phone
- Cisco Unified Communications Manager user to associate with the phone
- Phone usage information that affects phone button template, phone features, IP Phone services, or phone applications

The information provides a list of configuration requirements for setting up phones and identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates.

For more information, see the "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide*.

Step 2 Verify that you have sufficient unit licenses for your phone. For more information, see the "Licensing" section in the *Cisco Unified Communications Manager Features and Services Guide*.

Step 3 Customize phone button templates (if required) by changing the number of line buttons, speed-dial buttons or service URL buttons. Select **Device** > **Device Settings** > **Phone Button Template** to create and update the templates.
You can add a Privacy, All Calls, or Mobility button to meet user needs.

For more information, see the "Phone button template setup" chapter in the *Cisco Unified Communications Manager Administration Guide* and Phone Button Templates, on page 194.

Step 4 Define the Device Pools. Select **System** > **Device Pool**.
Device Pools define common characteristics for devices, such as region, date/time group, softkey template, and MLPP information. For information on Device Pool setup, see the "Device pool setup" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Define the Common Phone Profile. Select **Device** > **Device settings** > **Common Phone Profile**.
Common phone profiles provide data that the Cisco TFTP server requires, as well as common phone settings, such as Do Not Disturb and feature control options. For more information, see the "Common phone profile setup" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 6 Define a Calling Search Space. In Cisco Unified Communications Manager Administration, click **Call Routing** > **Class of Control** > **Calling Search Space**.
A Calling Search Space is a collection of partitions that are searched to determine how a dialed number is routed. The calling search space for the device and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS. For more information, see the "Calling search space setup" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Configure a security profile for the device type and protocol. Select **System** > **Security** > **Phone Security Profile**.
For more information, see the "Phone security profile setup" chapter in the *Cisco Unified Communications Manager Security Guide*.

Step 8 Add and configure the phone by completing the required fields in the Phone Configuration window. An asterisk (*) next to the field name indicates a required field; for example, MAC address and device pool.
This step adds the device with the default settings to the Cisco Unified Communications Manager database.

For more information, see the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

For information about product-specific configuration fields, see the "?" Button Help in the Phone Configuration window.

Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the "User/Phone Add Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 9 Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. An asterisk (*) next to the field name indicates a required field; for example, directory number and presence group.
This step adds primary and secondary directory numbers and features associated with directory numbers to the phone.

Note If you do not configure the primary directory number, the user sees the message `Unprovisioned` on the phone.

For more information, see the "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 10 Configure speed-dial buttons and assign speed-dial numbers.
Users can change speed-dial settings on their phones by using Cisco Unified Communications Self Care Portal.

For more information, see the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section in the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 11 Configure Cisco Unified IP Phone services and assign services (optional) to provide IP Phone services. Users can add or change services on their phones by using the Cisco Unified Communications Self Care Portal.

Note Users can subscribe to the IP Phone service only if the Enterprise Subscription check box is unchecked when the IP Phone service is first configured in Cisco Unified Communications Manager Administration.

Note Some Cisco-provided default services are classified as enterprise subscriptions, so the user cannot add them through the Self Care Portal. Such services are on the phone by default, and they can only be removed from the phone if you disable them in Cisco Unified Communications Manager Administration.

For more information, see the "IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 12 Assign services to programmable buttons (optional) to provide access to an IP Phone service or URL.
For more information, see the "Adding a Service URL Button" section of the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 13 Add user information by configuring required fields. An asterisk (*) next to the field name indicates a required field; for example, User ID and last name. This step adds user information to the global directory for Cisco Unified Communications Manager.

Note Assign a password (for Self Care Portal) and PIN (for Cisco Extension Mobility and Personal Directory).

For more information, see the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information about users, you can install and configure Cisco Unified Communications to use your existing LDAP directory.

Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the "User/Phone Add Configurations" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 14 Associate a user to a user group. This step assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For example, you must add users to the standard Cisco CCM End Users group so users can access Cisco Unified Communications Manager Self Care Portal.
For more information, see the following sections in the *Cisco Unified Communications Manager Administration Guide*:

- "End User Configuration Settings" section in the "End User Configuration" chapter
- "Adding Users to a User Group" section in the "User Group Configuration" chapter

Step 15 Associate a user with a phone (optional). This step provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services.
Some phones, such as those in conference rooms, do not have an associated user.

For more information, see the "Associating Devices to an End User" section in the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 16 If you are not already in the End User Configuration window, choose **User Management** > **End User** to perform some final configuration tasks. Use the Search fields and **Find** to locate the user (for example, John Doe), then click on the user ID to get to the End User Configuration window for the user.

Step 17 In the Directory Number Associations area of the screen, set the primary extension from the drop-down list.

Step 18 In the Mobility Information area, check the Enable Mobility box.

Step 19 In the Permissions Information area, use the User Group buttons to add this user to any user groups.
For example, you may want to add the user to a group that is defined as a Standard CCM End User Group.

Step 20 To view all configured user groups, choose **User Management** > **User Group**.

Step 21 In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user is allowed for Extension Mobility Cross Cluster service.

Step 22 Select **Save**.

Determine Phone MAC Address

To add phones to the Cisco Unified Communications Manager, you must determine the MAC address of a Cisco IP Phone.

Procedure

Perform one of the following actions:

- On the phone, press **Applications** > **Phone Information**, and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click **Device Information**.

Phone Addition Methods

After you install the Cisco IP Phone, you can choose one of the following options to add phones to the Cisco Unified Communications Manager database.

- Add phones individually using the Cisco Unified Communications Manager Administration
- Add multiple phones using the Bulk Administration Tool (BAT)
- Autoregistration
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

Adding phones individually or using BAT require you to identify the MAC address for the phone. For more information, see Determine Phone MAC Address, on page 70.

For more information about the Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Related Topics

Enable Autoregistration for Phone, on page 42

Add Phones Individually

Collect the MAC address and phone information for the phone that you will add to the Cisco Unified Communications Manager.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 Select the phone type.

Step 4 Select **Next**.

Step 5 Complete the information about the phone including the MAC Address.
For complete instructions and conceptual information about Cisco Unified Communications Manager, see the "Cisco Unified Communications Manager overview" chapter in the *Cisco Unified Communications Manager System Guide*.

Step 6 Select **Save**.

Add Phones Using BAT Phone Template

The Cisco Unified Communications Bulk Administration Tool (BAT) enables you to perform batch operations, including registration of multiple phones.

To add phones using BAT only (not in conjunction with TAPS), you must obtain the appropriate MAC address for each phone.

For detailed instructions about adding phones through the Bulk Administration menu, see the "Phone insertion" chapter of the *Cisco Unified Communications Manager Bulk Administration Guide*.

For more information about using BAT, see the *Cisco Unified Communications Manager Bulk Administration Guide*. For more information about creating of BAT Phone Templates, see the "Phone template" chapter in the *Cisco Unified Communications Manager Bulk Administration Guide*.

Procedure

Step 1 From Cisco Unified Communications Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.

Step 2 Click **Add New**.

Step 3 Choose a Phone Type and click **Next**.

Step 4 Enter the details of phone-specific parameters, such as Device Pool, Phone Button Template, Device Security Profile, and so on.

Step 5 Click **Save**.

Step 6 Select **Device** > **Phone** > **Add New** to add a phone using the BAT phone template.

Add Users to Cisco Unified Communications Manager

You can display and maintain information about the users registered in Cisco Unified Communications Manager. Cisco Unified Communications Manager also allows each user to perform tasks:

- Access the corporate directory and other customized directories from a Cisco IP Phone.
- Create a personal directory.
- Set up speed dial and call forwarding numbers.
- Subscribe to services that are accessible from a Cisco IP Phone.

Procedure

Step 1 To add users individually, see Add User Directly to Cisco Unified Communications Manager, on page 73.

Step 2 To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.
For more information, see the "Cisco Unified Communications Manager Bulk Administration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Add a User from an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize the LDAP directory to the Cisco Unified Communications Manager on which you are adding the user and the user phone.

Note If you do not synchronize the LDAP Directory to the Cisco Unified Communications Manager immediately, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next autosynchronization is scheduled. Synchronization must occur before you can associate a new user to a device.

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration.

Step 2 Select **System** > **LDAP** > **LDAP Directory**.

Step 3 Use **Find** to locate your LDAP directory.

Step 4 Click on the LDAP directory name.

Step 5 Click **Perform Full Sync Now**.

Add User Directly to Cisco Unified Communications Manager

If you are not using a Lightweight Directory Access Protocol (LDAP) directory, you can add a user directly with Cisco Unified Communications Manager Administration by following these steps.

Note If LDAP is synchronized, you cannot add a user with Cisco Unified Communications Manager Administration.

Procedure

Step 1 Choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 In the User Information pane, enter the following:

- User ID: Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces. **Example**: johndoe
- Password and Confirm Password: Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
- Last Name: Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces. **Example**: doe

- Telephone Number: Enter the primary directory number for the end user. End users can have multiple lines on their phones. **Example**: 26640 (John Doe's internal company telephone number)

Step 4 Click **Save**.

Add User to End User Group

To add a user to the Cisco Unified Communications Manager Standard End User group, perform these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **User Settings** > **Access Control Group**.
The Find and List Users window displays.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 Select the **Standard CCM End Users** link. The User Group Configuration window for the Standard CCM End Users appears.

Step 4 Select **Add End Users to Group**. The Find and List Users window appears.

Step 5 Use the Find User drop-down list boxes to find the users that you want to add and click **Find**.
A list of users that matches your search criteria appears.

Step 6 In the list of records that appear, click the check box next to the users that you want to add to this user group. If the list is long, use the links at the bottom to see more results.
Note The list of search results does not display users that already belong to the user group.

Step 7 Choose **Add Selected**.

Associate Phones with Users

You associate phones with users from the Cisco Unified Communications Manager End User window.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The Find and List Users window appears.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 In the list of records that appear, select the link for the user.

Step 4 Select **Device Association**.
The User Device Association window appears.

Step 5 Enter the appropriate search criteria and click **Find**.

Step 6 Choose the device that you want to associate with the user by checking the box to the left of the device.

Step 7 Choose **Save Selected/Changes** to associate the device with the user.

Step 8 From the Related Links drop-down list in the upper, right corner of the window, select **Back to User**, and click **Go**.
The End User Configuration window appears and the associated devices that you chose display in the Controlled Devices pane.

Step 9 Choose **Save Selected/Changes**.

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) ensures that basic phone functions remain accessible when communications with the controlling Cisco Unified Communications Manager are broken. In this scenario, the phone can keep an in-progress call active, and the user can access a subset of the features available. When failover occurs, the user receives an alert message on the phone.

The following table describes the availability of features during failover.

Table 11: SRST feature support

Feature	Supported	Notes
New Call	Yes	
End Call	Yes	
Redial	Yes	
Answer	Yes	
Hold	Yes	
Resume	Yes	
Conference	Yes	
Conference to Active Calls (Join)	No	The Active Calls softkey does not display.
Conference List	No	
Transfer	Yes	
Transfer to Active Calls (Direct Transfer)	No	
Auto Answer	Yes	

Feature	Supported	Notes
Call Waiting	Yes	
Caller ID	Yes	
Audible Message Waiting Indicator	Yes	
All Calls Programmable Line Key	Yes	
Answer Programmable Line Key	Yes	
Unified Session Presentation	Yes	Conference is the only feature supported due to other feature limitations.
Voicemail	Yes	Voicemail will not be synchronized with other users in the Cisco Unified Communications Manager cluster.
Call Forward All	Yes	Forward state is only available on the phone that sets the forward because there are no shared line appearances in SRST mode. The Call Forward All settings are not preserved on failover to SRST from the Cisco Unified Communications Manager, or from SRST fail-back to the Communications Manager. Any original Call Forward All still active on the Communications Manager should be indicated when the device reconnects to the Communications Manager after failover.
Speed Dial	Yes	
Service IRL Programmable Line Key	Yes	
To Voicemail (iDivert)	No	The iDivert softkey does not display.
Line Filters	Partial	Lines are supported but cannot be shared.
Park Monitoring	No	The Park softkey does not display.

Feature	Supported	Notes
Barge	No	The Merge softkey does not display.
Enhanced Message Waiting Indication	No	Message count badges do not appear on the phone screen. Only the Message Waiting icon displays.
Directed Call Park	No	The softkey does not display.
BLF	Partial	BLF feature key works like Speed Dial keys.
Hold Reversion	No	Calls remain on hold indefinitely.
Remote Hold	No	Calls appear as Local Hold calls.
Meet Me	No	The Meet Me softkey does not display.
PickUp	No	The softkey causes no action.
Group PickUp	No	The softkey causes no action.
Other PickUp	No	The softkey causes no action.
Malicious Call ID	No	The softkey causes no action.
QRT	No	The softkey causes no action.
Hunt Group	No	The softkey causes no action.
Intercom	No	The softkey causes no action.
Mobility	No	The softkey causes no action.
Privacy	No	The softkey causes no action.
Call Back	No	The Call Back softkey does not display.

Set Up Cisco Unified Communications Manager Features

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for Cisco IP Phones.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose one of the following windows:

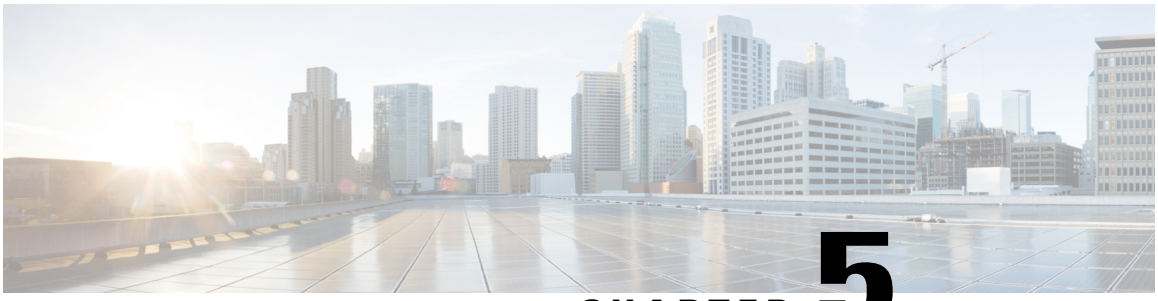
- **Device** > **Phone** (Phone Configuration window) Product Specific Configuration portion of window
- **Device** > **Device Settings** > **Common Phone Profile** (Common Phone Profile Configuration window)
- **System** > **Enterprise Phone Configuration** (Enterprise Phone Configuration window)

Step 2 Click the **?** button in Cisco Unified Communications Manager Administration for descriptions of the parameters.

Step 3 When you set the parameters, check the **Override Common Settings** check box for each setting that you wish to update.
If you do not check this box, the corresponding parameter setting does not take effect.

If you set the parameters in the three configuration windows, the setting takes precedence in the following order:

1. Phone Configuration window
2. Common Phone Profile window
3. Enterprise Phone Configuration window



CHAPTER 5

Self Care Portal Management

- Self Care Portal Overview, page 79
- Set Up Access to Self Care Portal, page 80
- Customize Self Care Portal Display, page 80

Self Care Portal Overview

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings. For information about the Self Care Portal, see the *Cisco Unified Communications Self Care Portal User Guide* located at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html.

As the administrator, you control access to the Self Care Portal. You must also provide information to your users so that they can access the Self Care Portal.

Before a user can access the Cisco Unified Communications Self Care Portal, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group.

You must provide end users with the following information about the Self Care Portal:

- The URL to access the application. This URL is:

  http://<server_name:portnumber>/ucmuser/, where server_name is the host on which the web server is installed and portnumber is the port number on that host.
- A user ID and default password to access the application.
- An overview of the tasks that users can accomplish with the portal.

These settings correspond to the values that you entered when you added the user to Cisco Unified Communications Manager.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, “Access Control Group Setup” chapter
- *Cisco Unified Communications Manager Administration Guide*, “End User Setup” chapter
- *Cisco Unified Communications Manager Administrator Guide*, “Role Setup” chapter

Set Up Access to Self Care Portal

Use this procedure to enable a user to access the Self Care Portal.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **User Management** > **End User**.
Step 2 Search for the user and click the user ID link.
Step 3 Ensure that the user has a password and PIN configured.
Step 4 Select **Save**.

Customize Self Care Portal Display

Most options display on the Self Care Portal. However, you must set the following options by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
- Show Line Label Settings

Note The settings apply to all Self Care Portal pages at your site.

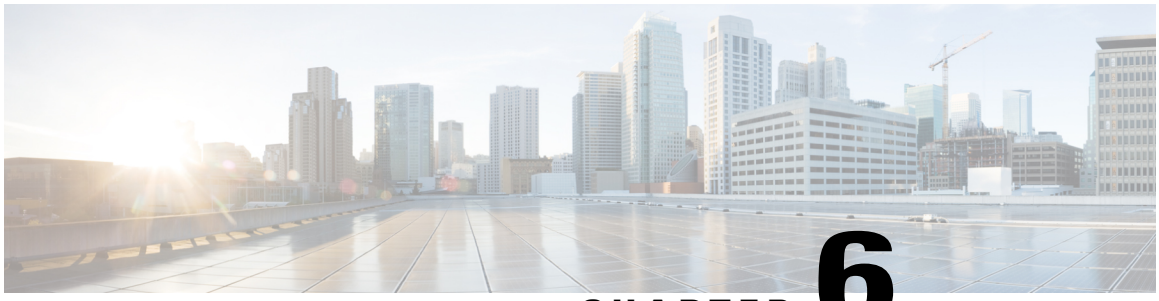
Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.
Step 2 In the Self Care Portal area, set the **Self Care Portal Default Server** field.
Step 3 Enable or disable the parameters that the users can access in the portal.
Step 4 Select **Save**.

PART III

Hardware and Accessory Installation

- Cisco IP Phone Accessories, page 83
- Cisco IP Phone Key Expansion Module, page 93
- Wall Mounts, page 109



CHAPTER 6

Cisco IP Phone Accessories

- Accessory Support, page 83
- Connect Footstand, page 84
- Secure the Phone with a Cable Lock, page 84
- External Speakers and Microphone, page 85
- Headsets, page 85

Accessory Support

The following table lists the accessories that the Cisco IP Phones 8811, 8841, 8851, and 8861 support. An "X" indicates support for a particular phone model and a dash (-) indicates no support.

Table 12: Accessory Support for the Cisco IP Phones 8811, 8841, 8851, and 8861

Accessory	Type	Cisco IP Phone 8811	Cisco IP Phone 8841	Cisco IP Phone 8851	Cisco IP Phone 8861
Cisco accessories					
Cisco IP Phone 8800 Key Expansion Module	Add-on module	-	-	X	X
Third-Party accessories					
Headsets: See Headsets, on page 85. This section includes information about each headset type.	Analog	X	X	X	X
	Analog Wideband	X	X	X	X
	Bluetooth	-	-	X	X
	USB (wired or wireless)	-	-	X	X

Accessory	Type	Cisco IP Phone 8811	Cisco IP Phone 8841	Cisco IP Phone 8851	Cisco IP Phone 8861
Microphone: See External Speakers and Microphone, on page 85.	External PC	-	-	-	X
Speakers: See External Speakers and Microphone, on page 85.	External PC	-	-	-	X

Connect Footstand

The phone includes an adjustable footstand. If the phone is placed on a table or desk, the footstand can be connected to the back of the phone. The footstand enables the phone angle to be adjusted from a minimum of 35 degrees to a maximum of 50 degrees to ensure an optimal viewing angle.

Note Adjusting the footstand to the required angle may require more force than you expect.

Procedure

Step 1 Insert the connectors into the slots provided.

Step 2 Press the footstand until the connectors snap into place.

Step 3 Adjust the angle by pressing down or pulling up on the footstand. The connectors are made of a flexible material.

Secure the Phone with a Cable Lock

You can secure the phone to a desktop with a laptop cable lock. The lock connects to the antitheft security connector on the back of the phone and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm wide. Compatible laptop cable locks include the Kensington laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.

Procedure

Step 1 Wrap the looped end of the cable lock and wrap it around object to which you want to secure your phone.

Step 2 Pass the lock through the looped end of the cable.

Step 3 Unlock the cable lock.

Note There are two kinds of cable locks: keyed and combination. Depending on the type of lock you have, unlock it by using the key or the correct combination.

Step 4 Press and hold the locking button to align the locking teeth.

Step 5 Insert the cable lock into the lock slot of your phone and release the locking button.

Step 6 Lock the cable lock.

Note For keyed locks, turn the key 90 degrees in the clockwise direction and pull the key out of the lock. For combination locks, rotate the lock 90 degrees and then scramble the combination.

External Speakers and Microphone

External speakers and microphones are plug-and-play accessories. You can connect an external PC-type microphone and powered speakers (with amplifier) on the Cisco IP Phone by using the line in/out jacks. Connecting an external microphone disables the internal microphone and connecting an external speaker disables the internal phone speaker.

Note Using poor quality external audio devices, playing loudspeakers at very loud volumes, or placing the microphone very close to the loudspeaker may result in undesirable echo for other parties on your speakerphone calls.

Headsets

Although Cisco Systems performs internal testing of third-party headsets for use with Cisco IP Phones, Cisco does not certify nor support products from headset or handset vendors.

The phone reduces some background noise that a headset microphone detects, but if you want to further reduce the background noise and improve the overall audio quality, use a noise cancelling headset.

Cisco recommends the use of good quality external devices, for example, headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of headsets and their proximity to other devices, such as mobile (cell) phones and two-way radios, some audio noise or echo may still occur. Either the remote party or both the remote party and the Cisco IP Phone user may hear an audible hum or buzz. A range of outside sources can cause humming or buzzing sounds; for example, electric lights, electric motors, or large PC monitors.

Note In some cases, using a local power cube or power injector may reduce or eliminate hum.

These environmental and hardware inconsistencies in the locations where Cisco IP Phones are deployed mean that no single headset solution is optimal for all environments.

Cisco recommends that customers test headsets in the intended environment to determine performance before making a purchasing decision and deploying on a large scale.

Related Topics

External Devices, on page 16

Audio Quality

Beyond physical, mechanical, and technical performance, the audio portion of a headset must sound good to the user and to the party on the far end. Sound quality is subjective and Cisco cannot guarantee the performance of any headsets. However, a variety of headsets from leading headset manufacturers are reported to perform well with Cisco IP Phones.

For additional information, see http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html

Analog Headsets

The phone cannot detect when an analog headset is plugged in. For this reason, the analog headset displays by default in the Accessories window on the phone screen.

Displaying the analog headset as the default allows users to enable wideband for the analog headset.

Enable Wideband on Analog Headsets

Although analog headsets are supported on the phone, the phones cannot detect when an analog headset is plugged in. For this reason, by default, the analog headset displays in the Accessories window on the phone screen.

Displaying the analog headset as the default allows users to enable wideband for the analog headset.

The phone is unable to detect whether the headset supports the wideband codec, but the user can enable wideband on analog headsets by following these steps:

Procedure

Step 1 On the Cisco IP Phone, press **Applications** .

Step 2 Select **Accessories**.

Step 3 Highlight the analog headset, then press **Setup**.

Step 4 Press **On** to turn on the wideband and press **Off** to turn off the wideband.

Enable Wideband Codec on Analog Headsets

Although analog headsets are supported on the phone, the phones cannot detect when an analog headset is plugged in. For this reason, by default, the analog headset displays in the Accessories window on the phone screen.

Displaying the analog headset as the default allows users to enable wideband for the analog headset.

If the screen doesn't display On or Off softkey, follow these steps to ensure that the user can enable wideband codec on an analog headset:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 In the Find and List Phones window, enter the search criteria for the phone to which you want to add the analog headset, then click **Find**.

Step 3 Click on the Device Name that you want. The Phone Configuration window displays.

Step 4 On the Product Specific Configuration Layout portion of the Phone Configuration window, ensure that the Wideband Headset UI Control option is enabled. (This option is enabled by default.)

Step 5 In the Product Specific Configuration Layout portion of the Phone Configuration window, you can also set the Wideband Headset option. (This option is also enabled by default).

Wired Headsets

You can use the wired headset with all of the features on the Cisco IP Phone, including the Volume and Mute buttons. Use these buttons to adjust the earpiece volume and to mute the speech path from the headset microphone.

Connect Wired Headset

To connect a wired headset to the Cisco IP Phone, perform these steps:

Procedure

Step 1 Plug the headset into the Headset port on the back of the phone.

Step 2 Press the **Headset** button on the phone to place and answer calls using the headset.

Disable Wired Headset

You can disable the headset by using Cisco Unified Communications Manager Administration. If you do so, you also disable the speakerphone.

Procedure

Step 1 To disable the headset from Cisco Unified Communications Manager Administration, choose **Device** > **Phone** and locate the phone that you want to modify.

Step 2 In the Phone Configuration window (Product Specific Configuration layout portion), select the **Disable Speakerphone and Headset** check box.

USB Headsets

Wired and wireless USB headsets are supported. You can connect a USB headset (or the base station for a wireless headset) to either the back USB port (if your phone has this port) or to the side USB port.

For a list of supported headsets, see http://www.cisco.com/c/en/us/products/unified-communications/ucphone_headsets.html.

Enable USB Headset

You must enable the applicable USB port (either the back USB port parameter or the side USB port parameter) in Cisco Unified Communications Manager Administration (in the Product Specific Configuration layout portion of the window). Also, for the Enable/Disable USB Classes parameter in Cisco Unified Communications Manager Administration, ensure that Audio Class is selected.

Procedure

Step 1 Enable the USB headset in one of the following windows:

- Phone Configuration (**Device** > **Phone**).
- Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**).
- Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**).

Step 2 Check the corresponding Override Common Settings parameter in the configuration window.

Disable USB Headset

To disable the USB headset, disable the USB port (or disable the Audio Class parameter) that you enabled in Cisco Unified Communications Manager Administration. Also, you can select another type of headset in the Accessories window on the phone, thus disabling the previously enabled headset.

Procedure

Step 1 Disable the USB headset in one of the following windows:

- Phone Configuration (**Device** > **Phone**).
- Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**).
- Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**).

Step 2 Check the corresponding Override Common Settings parameter in the configuration window.

Wireless Headsets

You can use a wireless headset with the Cisco IP Phone.

The Cisco website provides information about wireless headsets that work with your IP phone. Go to the following URL:

http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html

See the wireless headset documentation for information about connecting the headset and using the features.

Enable Electronic Hookswitch

The Electronic Hookswitch feature supports the following headset devices:

- Jabra
  - PRO9400 and GO6400 series
  - PRO930
  - GN9300 series
  - GN9120
- Plantronics
  - Savi DECT 740, CS5xx DECT

Procedure

Step 1 From the Cisco Unified Communications Manager Administration, choose **Device** > **Phone**

Step 2 Scroll to the Wireless Headset Hookswitch Control section

Step 3 Choose **Enable** or **Disable**.

Bluetooth Wireless Headsets

For a list of supported headsets, see http://www.cisco.com/c/en/us/products/unified-communications/ucphone_headsets.html.

Bluetooth enables low-bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3- to 6-foot (1- to 2-meter) range. Bluetooth wireless technology operates in the 2.4 GHz band, which is the same as the 802.11b/g band. Interference issues can occur. Cisco recommends that you:

- Use 802.11a, 802.11n or 802.11ac that operates in the 5 GHz band.
- Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.

The Cisco IP Phone uses a shared key authentication and encryption method to connect with headsets. The Cisco IP Phone can connect with up to fifty headsets, one at a time. The last connected headset is used as the default. Pairing is typically performed once for each headset.

After a device is paired, the Bluetooth connection is maintained as long as both devices (phone and headset) are enabled and within range of each other. The connection typically reestablishes itself automatically if either of the devices powers down then powers up. However, some headsets require user action to reestablish the connection.

The Bluetooth icon indicates that Bluetooth is on irrespective of whether a device is connected or not.

Potential interference issues can occur. Cisco recommends that you reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects. If possible, configure other 802.11 devices to use the 802.11a channels.

For a Bluetooth wireless headset to work, it does not need to be within direct line-of-sight of the phone, but some barriers, such as walls or doors, and interference from other electronic devices, can affect the connection.

When headsets are more than 30 feet (10 meters) away from the Cisco IP Phone, Bluetooth drops the connection after a 15- to 20-second timeout. If the paired headset comes back into range of the Cisco IP Phone and the phone is not connected to another Bluetooth headset, the in-range Bluetooth headset automatically reconnects. For certain phone types that operate in power-save modes, the user can wake up the headset by tapping on the operational button to initiate the reconnect.

You must enable the headset and then add it as a phone accessory.

The phone supports various Handsfree Profile features that enable you to use hands-free devices (such as Bluetooth wireless headsets) to perform certain tasks without having to handle the phone. For example, instead of pressing Redial on the phone, users can redial a number from their Bluetooth wireless headset by following instructions from the headset manufacturer.

These hands-free features apply to Bluetooth wireless headsets that are used with the Cisco IP Phone 8851 and 8861:

- Answer a call
- End a call
- Change the headset volume for a call
- Redial
- Caller ID
- Divert
- Hold and Accept
- Release and Accept

Hands-free devices may differ as to how features are activated. Device manufacturers may also use different terms when referring to the same feature.

Important Only one headset type works at any given time, so if you use both a Bluetooth headset and an analog headset that are attached to the phone, enabling the Bluetooth headset disables the analog headset. To enable the analog headset, disable the Bluetooth headset. Plugging a USB headset into a phone that has Bluetooth headset enabled disables both the Bluetooth and analog headset. If you unplug the USB headset, you can either enable the Bluetooth headset or disable the Bluetooth headset to use the analog headset.

For information about how to use your Bluetooth wireless headset, see:

- *Cisco IP Phone 8811, 8841, 8851, and 8861 User Guide for Cisco Unified Communications Manager*
- User guides provided with your headset

Enable Bluetooth Wireless Headset

Before users can use a Bluetooth Wireless headset, you must enable it.

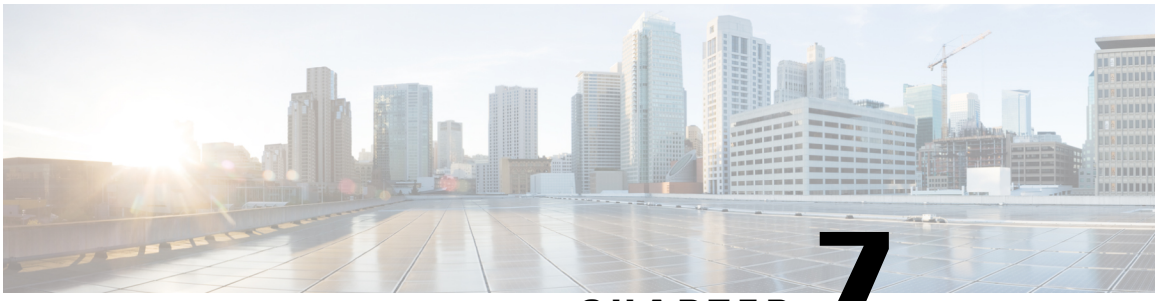
Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Locate the phone you want to modify, and go to the Phone Configuration window for that phone.

Step 3 In the Phone Configuration window, select **Enable** for the Bluetooth setting and **Handsfree** for the Bluetooth Profiles setting.

Step 4 Save your changes.



CHAPTER 7

Cisco IP Phone Key Expansion Module

- Cisco IP Phone Key Expansion Module Setup Overview, page 93
- KEM Power Information, page 94
- Connect Single KEM to Cisco IP Phone, page 95
- Connect Two or Three KEMs to Cisco IP Phone, page 99
- Set Up Key Expansion Module in Cisco Unified Communications Manager Administration, page 103
- Access Key Expansion Module Setup, page 105
- Reset Key Expansion Module, page 106
- Troubleshoot the Key Expansion Module, page 106

Cisco IP Phone Key Expansion Module Setup Overview

The Cisco IP Phone 8800 Key Expansion Module (KEM) adds additional line appearances, speed dials, or programmable buttons to the phone. The programmable buttons can be set up as phone line buttons, speed-dial buttons, or phone feature buttons

The following table lists the phones and the number of Key Expansion Modules that each model supports.

Table 13: Cisco IP Phones and Supported KEMs

Cisco IP Phone model	Supported KEMs
Cisco IP Phone 8851	2 KEMs with 72 lines or buttons
Cisco IP Phone 8861	3 KEMs with 108 lines or buttons

Related Topics

Wall Mounts, on page 109

KEM Power Information

The Cisco IP Phone 8800 Key Expansion Module possesses the following power consumption and power scheme:

Power consumption

48V DC, 5W per KEM

Power scheme

The phone can power one KEM directly. For more information, see the following table.

Table 14: Key Expansion Module Power

	Cisco IP Phone 8851			Cisco IP Phone 8861		
Accessories	**802.3af PoE**	**802.3at PoE**	**Cisco IP Phone Power Cube 4**	**802.3af PoE**	**802.3at PoE**	**Cisco IP Phone Power Cube 4**
1 KEM	Supported	Supported	Supported	Not supported	Supported	Supported
2 KEM	Not supported	Not supported	Supported	Not supported	Supported	Supported
3 KEM	Not supported	Not supported	Not supported	Not supported	Supported	Supported
1 KEM + tablet charging	Not supported	Not supported	Not supported	Not supported	Supported	Supported
2 KEM + tablet charging	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
3 KEM + tablet charging	Not supported	Not supported	Not supported	Not supported	Not supported	Supported

Note When more than one KEM is attached to the Cisco IP Phone 8861, the fast-charge feature using the back USB port is not supported. In this scenario, the back port will slow-charge the device.

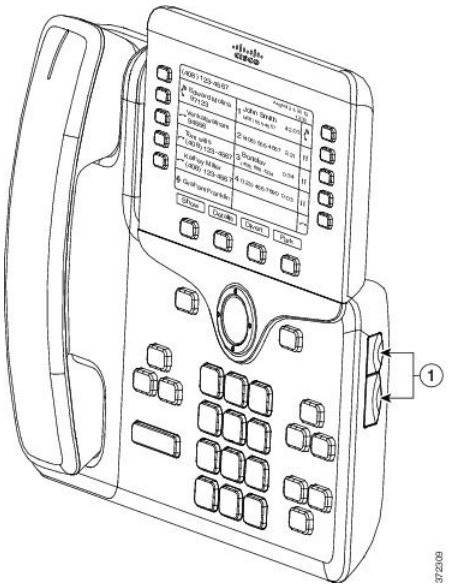
Connect Single KEM to Cisco IP Phone

Procedure

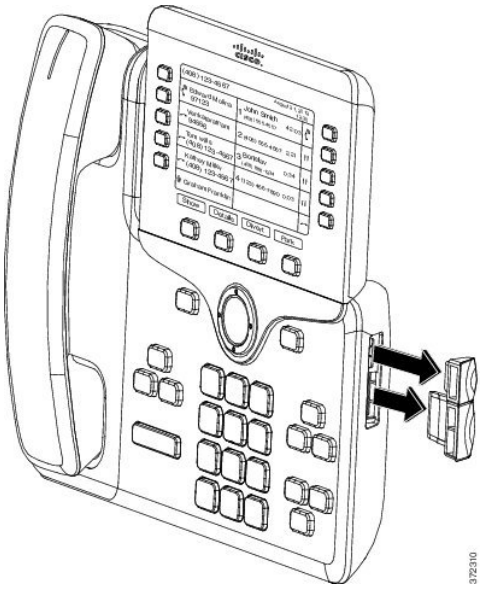
Step 1 Unplug the Ethernet cable from the phone.

Step 2 If installed, remove the footstand from the phone.

Step 3 Locate the accessory connector covers on the side of the phone.
The following diagram shows the location of the accessory connector covers.



Step 4 Remove the two accessory connector covers.
The following diagram shows the removal of an accessory connector cover.



Attention The slots are designed for the spine connector only. Inserting other objects will cause permanent damage to the phone.

Step 5 Position the phone so that the front of the phone is facing up.

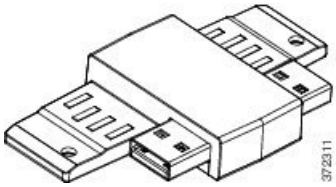
Step 6 Connect one end of the KEM spine connector to the accessory connector on the Cisco IP Phone.

a) Align the spine connector with the accessory connector ports.

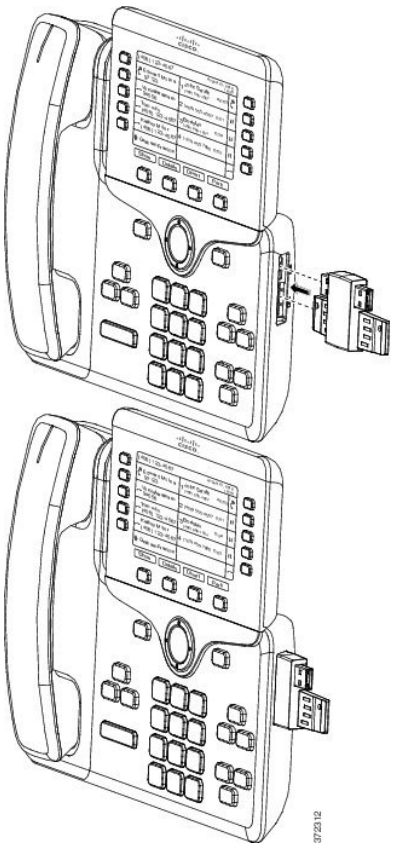
Note Install the connector in the orientation shown in the following diagrams.

b) Firmly press the spine connector into the phone.

The following diagram shows the spine connector.



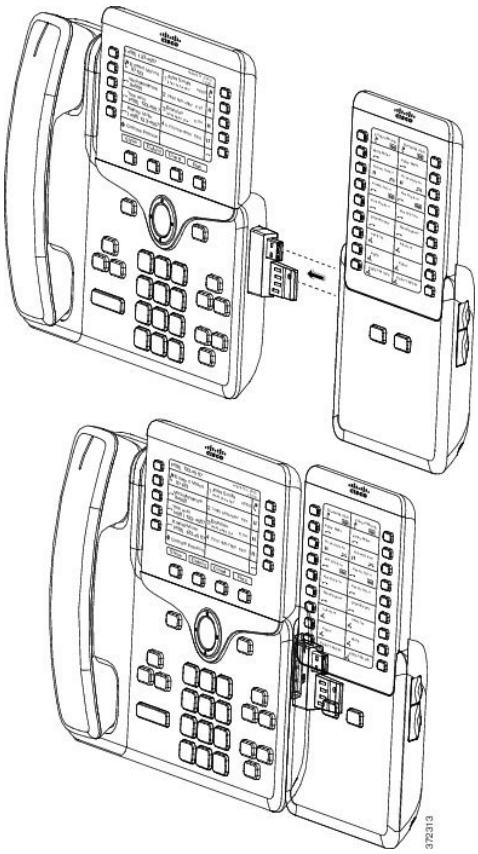
The following diagram shows the installation of the spine connector.



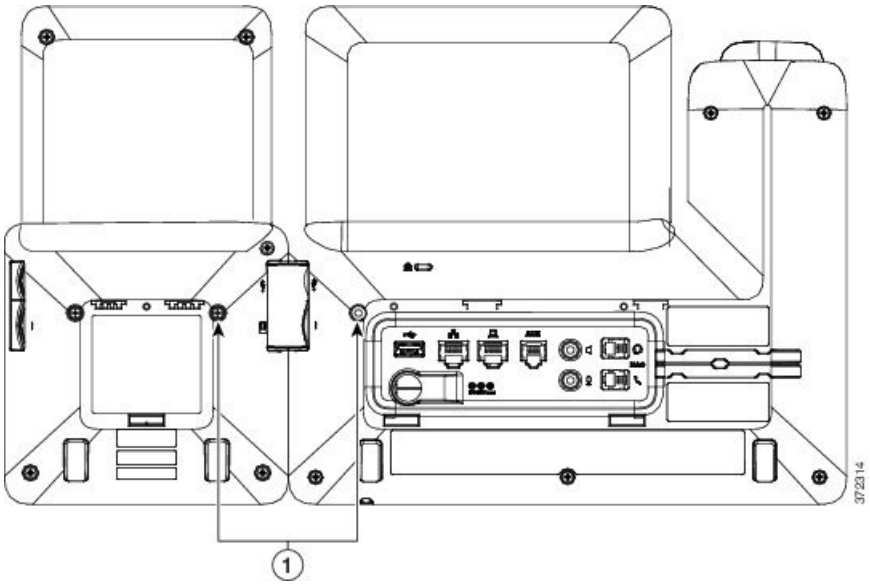
Step 7 Connect the other end of the spine connector to the KEM as shown in the following figure.

a) Align the spine connector with the KEM accessory connector ports.

b) Firmly press the KEM into the spine connector.



Step 8 Use a screwdriver to fasten the screws into the phone.
This step ensures that the phone and KEM remain connected at all times. The following diagram shows the location of the screw holes on the phone and one KEM.



Note Make sure that the screws fully inserted into the phone and tightened.

Step 9 (Optional) Install the footstands on the phone and on the KEM, and adjust both footstands to rest evenly on the work surface.

Step 10 Plug the Ethernet cable into the phone.

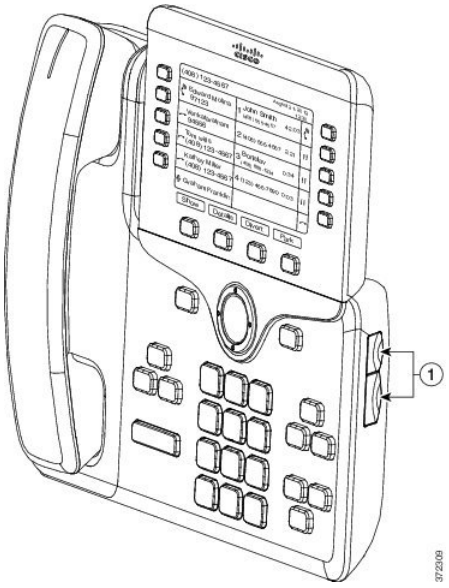
Connect Two or Three KEMs to Cisco IP Phone

Procedure

Step 1 Unplug the Ethernet cable from the phone.

Step 2 If installed, remove the footstand from the phone.

Step 3 Locate the accessory connector covers on the side of the phone.
The following diagram shows the location of the accessory connector covers.



Step 4 Remove the two accessory connector covers.
The following diagram shows the removal of an accessory connector cover.

Attention The slots are designed for the spine connector only. Inserting other objects will cause permanent damage to the phone.

Step 5 Position the phone so that the front of the phone is facing up.

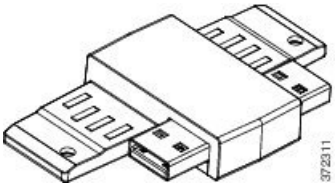
Step 6 Connect one end of the KEM spine connector to the accessory connector on the Cisco IP Phone.

a) Align the spine connector with the accessory connector ports.

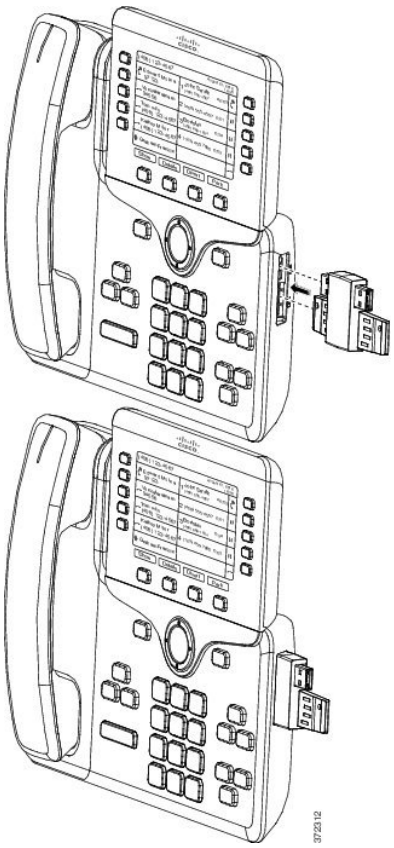
Note Install the connector in the orientation shown in the following diagrams.

b) Firmly press the spine connector into the phone.

The following diagram shows the spine connector.



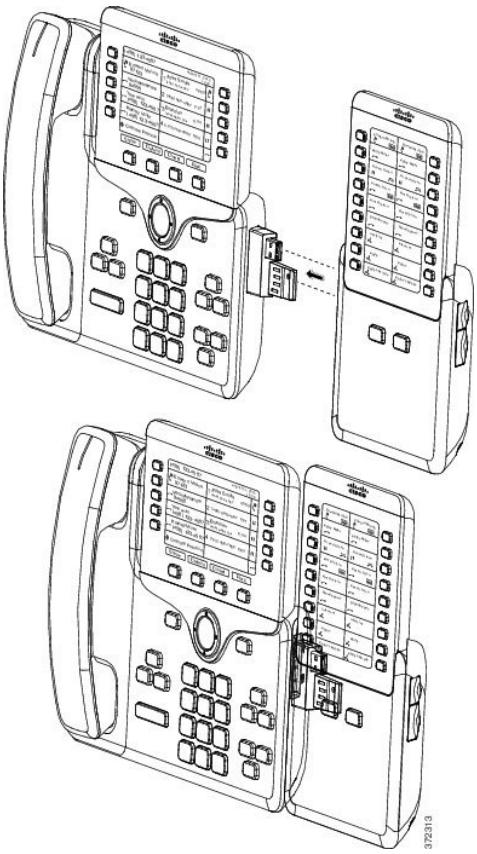
The following diagram shows the installation of the spine connector.



Step 7 Connect the other end of the spine connector to the KEM as shown in the following figure.

a) Align the spine connector with the KEM accessory connector ports.

b) Firmly press the KEM into the spine connector.

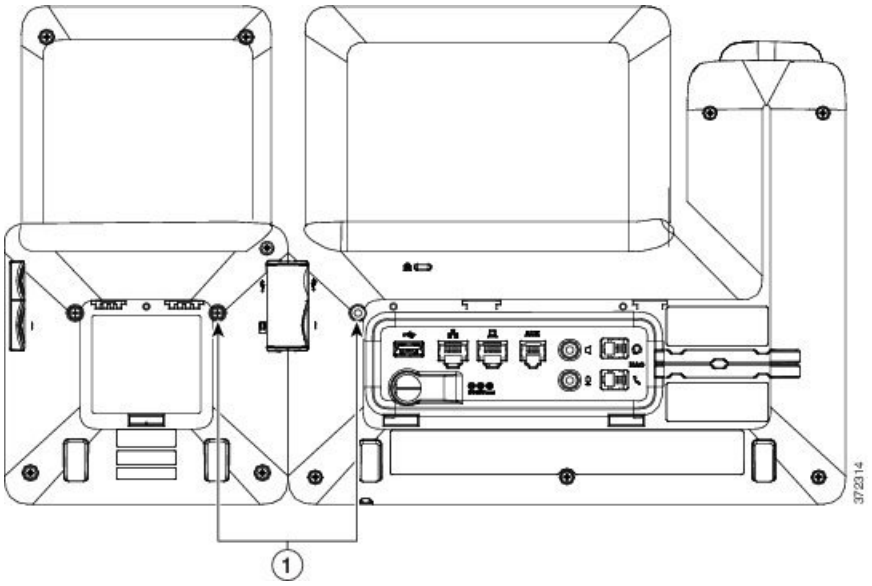


The first KEM is now connected to the Cisco IP Phone.

Step 8 Use a second KEM spine connector to connect the second KEM to the first KEM.

Step 9 Use a third KEM spine connector to connect the third KEM to the second (middle) KEM. The following figure shows a Cisco IP Phone with three KEMs attached.

Step 10 Use a screwdriver to fasten the screws into the phone and each KEM.
This step ensures that the phone and KEMs remain connected at all times. The following diagram shows the location of the screw holes.



Note Make sure that the screws fully inserted into the phone and tightened.

Step 11 (Optional) Install the footstands on the phone and on the KEMs, and adjust all footstands to rest evenly on the work surface.

Step 12 Plug the Ethernet cable into the phone.

Set Up Key Expansion Module in Cisco Unified Communications Manager Administration

During the Key Expansion Module setup, you can configure the KEM to display on one-column or two-column mode.

One-column mode

In one-column mode, each row in the display corresponds to one line, and this line can be accessed by either the button on the left or the button on the right. In this configuration, the Key Expansion Module displays 9 lines on page 1, and 9 lines on page 2. The following graphic shows the one-column mode.

Two-column mode

In two-column mode, each of the buttons on the left and right of the screen is assigned to different lines. In this configuration, the Key Expansion Module displays 18 lines on page 1, and 18 lines on page 2. The following graphic shows the two-column mode.

Note If the label is longer than the display space in both one- and two-column mode, the text contains an ellipsis (…) .

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.
The Find and List Phones window appears. You can search for one or more phones that you want to configure for the Cisco IP Phone 8800 Key Expansion Module.

Step 2 Select and enter your search criteria and click **Find**.
The Find and List Phones window appears with a list of phones that match your search criteria.

Step 3 Click the phone that you want to configure for the Cisco IP Phone 8800 Key Expansion Module. The Phone Configuration window appears.

Step 4 Scroll down to the Expansion Module Information section on the right pane of the Phone Configuration window, and choose the appropriate expansion module (or "none") for the Module 1, Module 2 and Module 3 fields, in that order.
For the number of supported KEMs per phone model, see Cisco IP Phone Key Expansion Module Setup Overview, on page 93.

Step 5 Be sure to select the phone button template (in the Device Information portion of the Phone Configuration window) that is configured to make full use of the KEMs attached to the phone.

Step 6 Depending on your requirements, enable the One Column Display for KEM field for one-column mode, or disable the field for two-column mode.

Step 7 Click **Save**.

Access Key Expansion Module Setup

After you install one or more KEMs on the phone and configure them in Cisco Unified Communications Manager Administration, the KEMs are automatically recognized by the phone.

When multiple KEMs are attached, they are numbered according to the order in which they connect to the phone:

- Key Expansion Module 1 is the KEM closest to the phone.
- Key Expansion Module 2 is the KEM in the middle.
- Key Expansion Module 3 is the KEM farthest to the right.

You can select a KEM, and then choose one of the following softkeys:

- Exit: Returns to the Applications menu.
- Details: Provides details about the selected KEM.

- Setup: Allows you to configure the brightness of the selected KEM. Setting the brightness can also be done using the Preferences menu on the phone. For details, see the *Cisco IP Phone 8841, 8851, and 8861 User Guide for Cisco Unified Communications Manager (SIP)*.

Procedure

Step 1 On the phone, press **Applications** .

Step 2 Press **Accessories**.
All properly installed and configured KEMs display in the list of accessories.

Reset Key Expansion Module

This procedure gives the steps for the Key Expansion Module factory reset.

Procedure

Step 1 Power on the KEM, press **Page 1**, and do not release the key. When the LCD turns white, continue pressing **Page 1** for at least one second.

Step 2 Release **Page 1**; LEDs should turn red. Immediately press **Page 2** and continue pressing **Page 2** for at least one second.

Step 3 Release **Page 2**; all LEDs should turn amber.

Step 4 Press Lines **5**, **14**, **1**, **18**, **10**, and **9** in sequence.
The LCD should turn blue, and the spinning loader icon displays in the center.

The KEM resets.

Troubleshoot the Key Expansion Module

To obtain Key Expansion Module (KEM) troubleshooting information, follow these steps:

Procedure

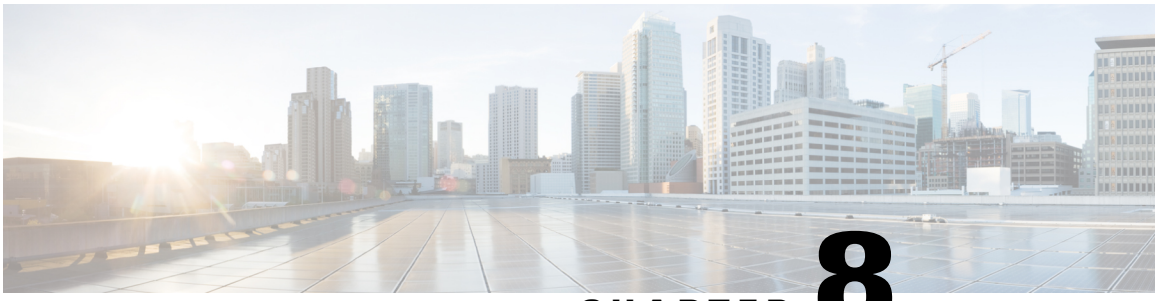
Step 1 Open a CLI.

Step 2 Enter the following command to enter debug mode:
debugsh

Step 3 Enter **?** to see all available commands and options.

Step 4 Use the applicable commands and options to find the desired KEM information.

Step 5 To exit debug mode, press **Ctrl-C**.



CHAPTER 8

Wall Mounts

- Wall Mount Options, page 109
- Non-Lockable Wall Mount Components for Phone, page 109
- Non-Lockable Wall Mount Components for Phone with Key Expansion Module, page 116
- Adjust the Handset Rest, page 122

Wall Mount Options

You can mount the phone on the wall by using special brackets that are available in a Cisco IP Phone wall mount kit. Wall mount kits must be ordered separately from the phone.

The following wall mount options are available:

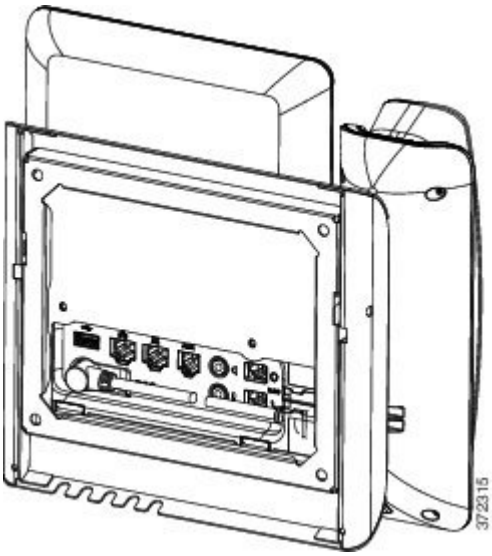
- Cisco IP Phone 8800 Series Wall Mount Kit: A nonlockable wall mount kit for the Cisco IP Phones 8811, 8841, 8851, and 8861.
- Cisco IP Phone 8800 Series Wall Mount Kit with Single KEM: A nonlockable wall mount kit installed on the Cisco IP Phone 8851 and 8861 with one attached Cisco IP Phone 8800 Key Expansion Module.

Non-Lockable Wall Mount Components for Phone

This section describes how to install the Cisco IP Phone 8800 Series Wall Mount Kit.

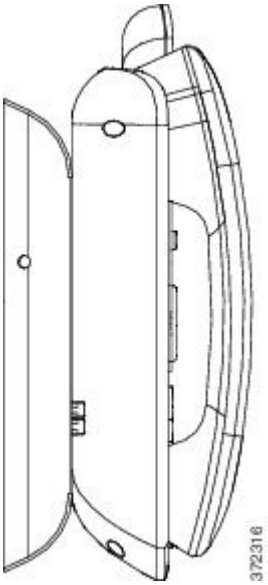
The following figure shows the wall mount kit installed on the phone.

Figure 1: Back view of Wall Mount Kit Installed on Phone



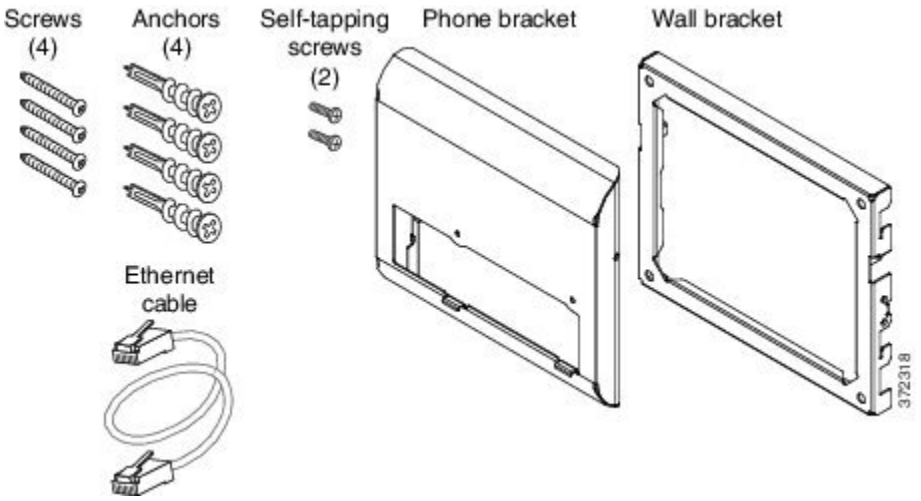
The following figure shows the phone with the wall mount kit from the side.

Figure 2: Side View of Wall Mount Kit Installed on Phone



The following figure shows the components of the Cisco IP Phone 8800 Series Wall Mount Kit.

Figure 3: Components



The package contains the following items:

- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two K30x8mm self-tapping screws
- One 6-inch Ethernet cable

Install the Non-Lockable Wall Mount Kit for Phone

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack.

Procedure

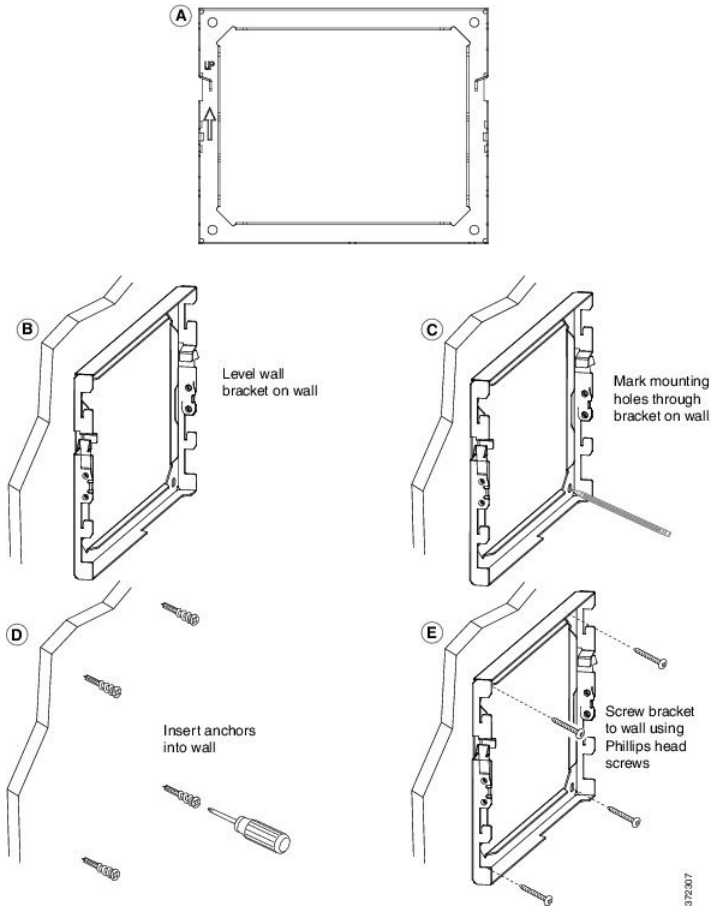
Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

Note If the jack is to be placed behind the phone, the Ethernet jack must be flush to the wall or recessed.

a) Hold the bracket on the wall, placing it so that the arrow on the back of the bracket is pointing up.
b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
c) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
d) Screw the anchor clockwise into the wall until it is seated flush.
e) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the bracket installation steps.

Figure 4: Bracket Installation



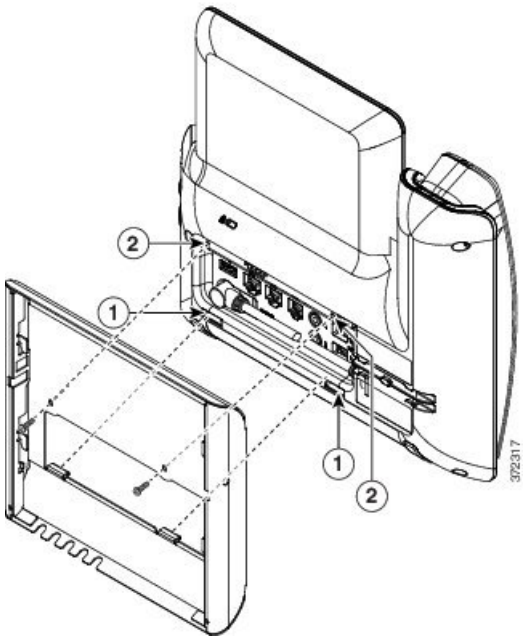
Step 2 Attach the phone bracket to the IP Phone.

a) Detach power cord, and any other attached cords from the base of the phone, except the handset cord (and headset cord, if there is a headset).

b) Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.
c) Secure the phone bracket to the IP phone with the self-tapping screws, using the #1 Phillips-head screwdriver.
d) Reattach the cords and seat them in the clips that are incorporated into the phone body.

The following figure shows how the bracket attaches to the phone.

Figure 5: Attach Phone Bracket

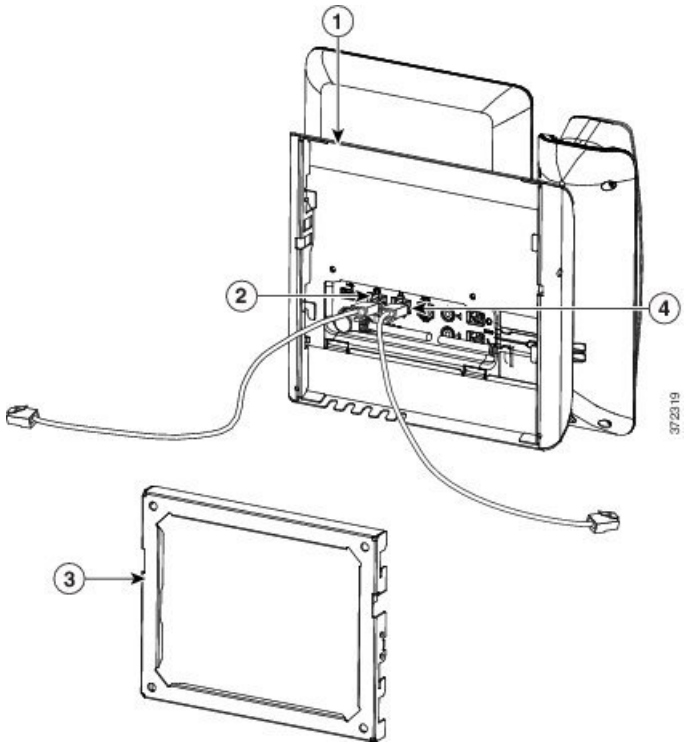


Step 3 Attach the cables to the phone:

a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.
b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.
c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.
d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cables.

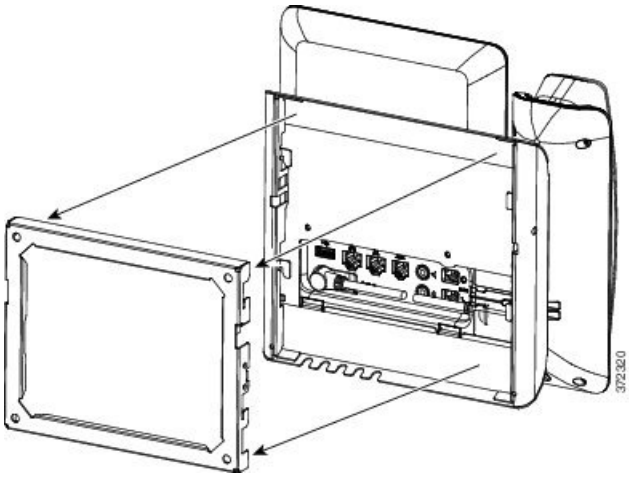
Figure 6: Attach Cables



Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the wall bracket into the slots on the phone bracket.
For cables that terminate outside of the brackets, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

The following figure shows how you attach the phone to the wall bracket.

Figure 7: Attach Phone to Wall Bracket



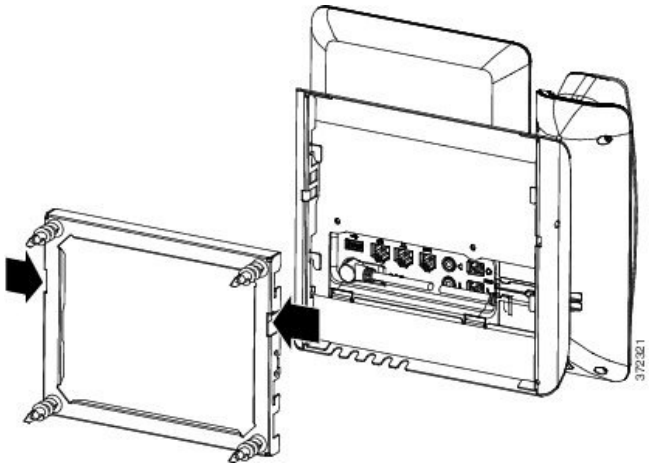
Step 5 Press the phone firmly into the wall bracket and slide the phone down. The tabs in the bracket click into position.

Step 6 Proceed to Adjust the Handset Rest, on page 122.

Remove the Phone from the Non-Lockable Wall Mount

The wall bracket contains two tabs to lock the plate into the phone mounting plate. The following figure shows the location and shape of the tabs.

Figure 8: Tab Location



To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

Before You Begin

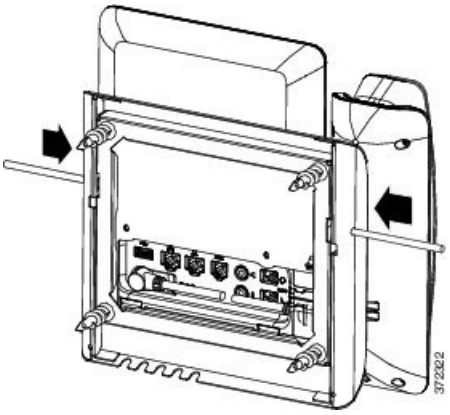
You require 2 metal rods.

Procedure

Step 1 Push the rods into the left and right holes in the phone mounting plate approximately 0.75 in (2.0 cm).

Step 2 Press firmly inwards (towards the phone) to disengage the tabs, lift up on the phone to release the phone from the wall bracket, and then pull the phone towards you.

Figure 9: Disengage Tabs

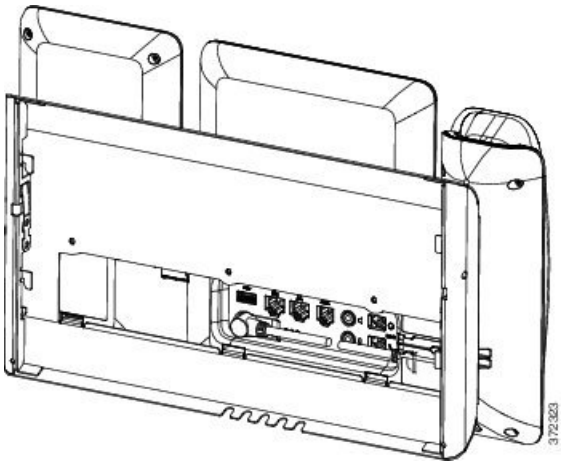


Step 3 Press firmly to disengage the tabs and lift the phone at the same time to release the phone from the wall bracket.

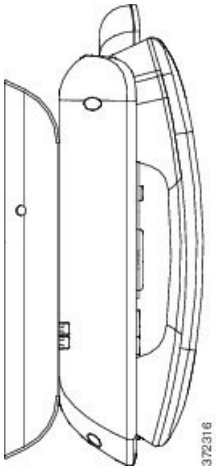
Non-Lockable Wall Mount Components for Phone with Key Expansion Module

This section describes how to install the Cisco IP Phone 8800 Series Wall Mount Kit with Single KEM on a phone when the phone is connected to a Key Expansion Module.

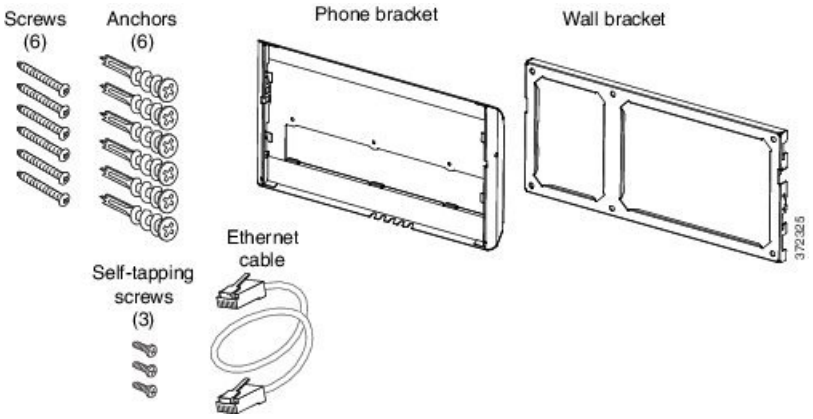
The following figure shows the wall mount kit installed on the phone.



The following figure shows the phone with the wall mount kit from the side.



The following figure shows the components of the Cisco IP Phone 8800 Series Wall Mount Kit with Single KEM.



The package contains the following items:

- One phone bracket
- One wall bracket

- Six #8-18 x 1.25-inch Phillips-head screws with six anchors
- Three K30x8mm self-tapping screws
- One 6-inch Ethernet cable

Install Non-Lockable Wall Mount Kit for Phone with Key Expansion Module

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

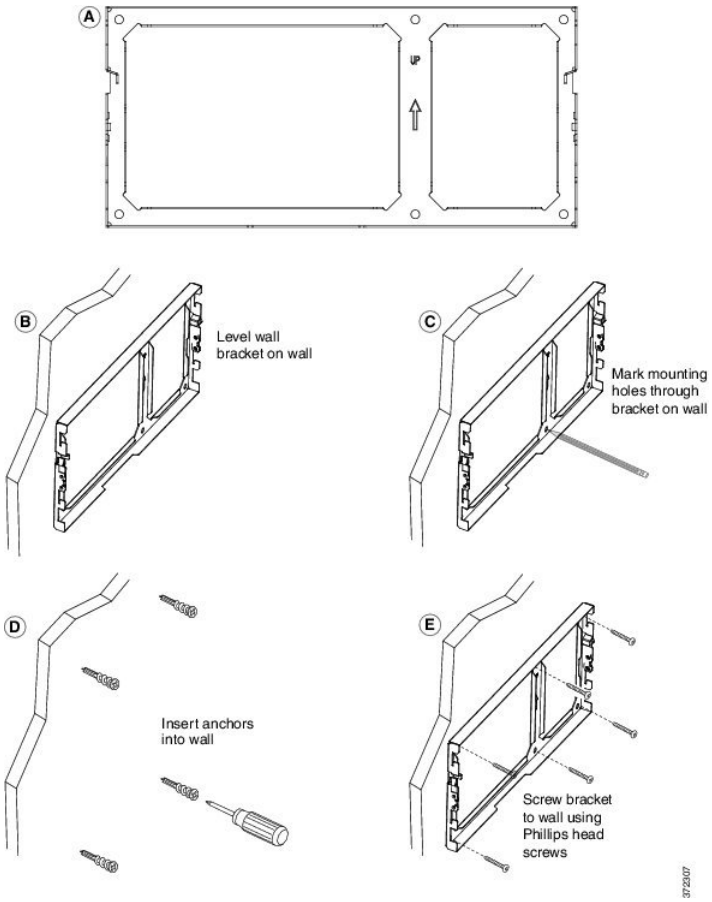
You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack.

Procedure

Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

Note If the jack is to be placed behind the phone, the Ethernet jack must be flush to the wall or recessed.

a) Hold the bracket on the wall. See the following figure for the orientation of the wall bracket.
b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
c) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
d) Screw the anchor clockwise into the wall until it is seated flush.
e) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.



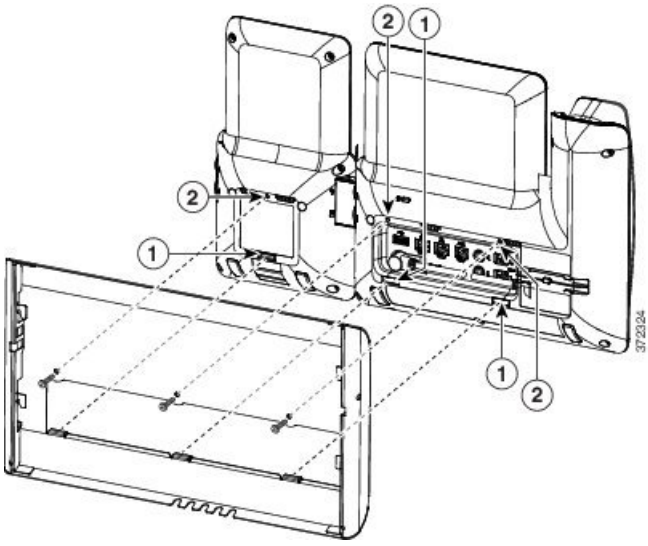
Step 2 Attach the phone bracket to the IP phone and key expansion assembly.

a) Detach power cord, and any other attached cords from the base of the phone, except the handset cord (and headset cord, if there is a headset).

b) Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.

c) Secure the phone bracket to the IP phone with the self-tapping screws using a #1 Philips-head screwdriver.

d) Reattach the cords and seat them in the clips that are incorporated into the phone body.



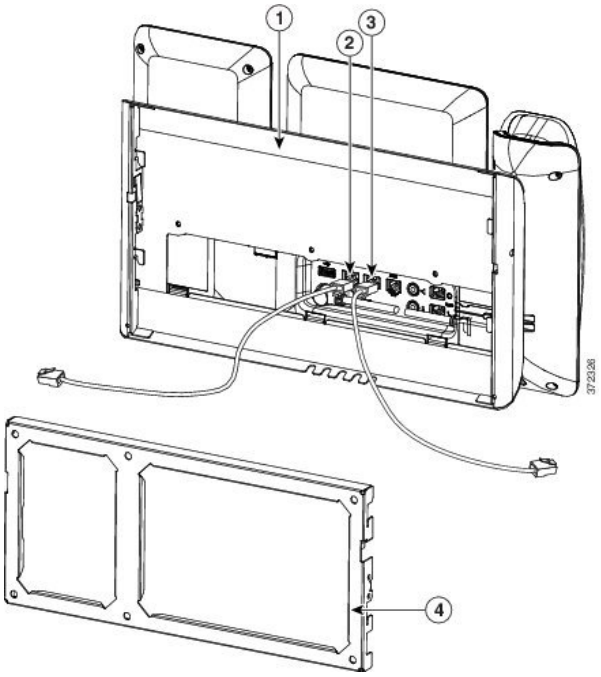
Step 3 Attach the cords.

a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

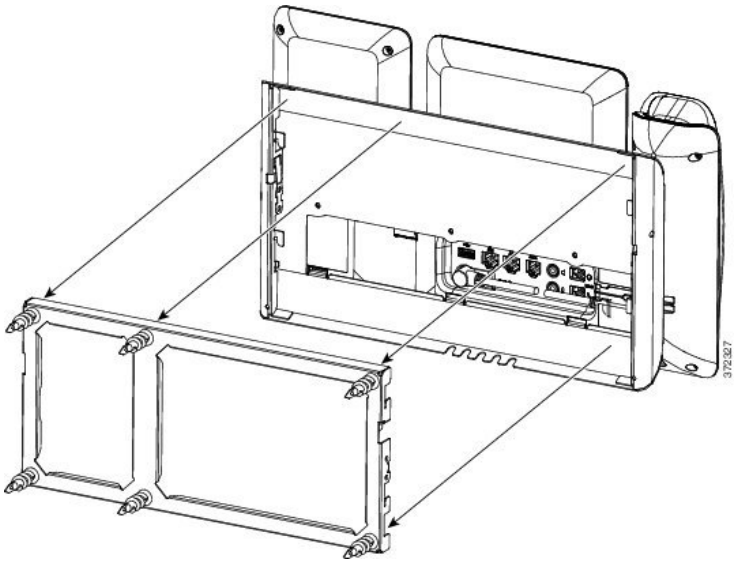
c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.



Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.

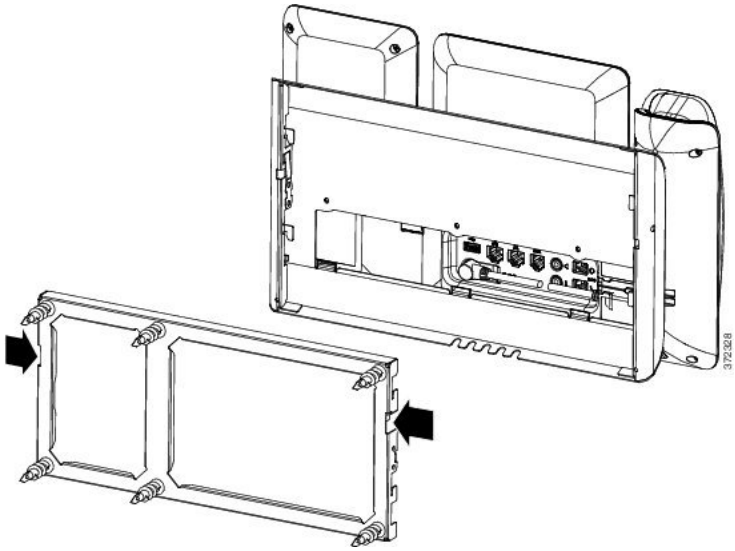
For cables that terminate outside of the bracket, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.



Step 5 Proceed to Adjust the Handset Rest, on page 122.

Remove the Phone and Key Expansion Module from the Non-Lockable Wall Mount

The wall bracket contains two tabs to lock the plate into the phone mounting plate. The following figure shows the location and shape of the tabs.



To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

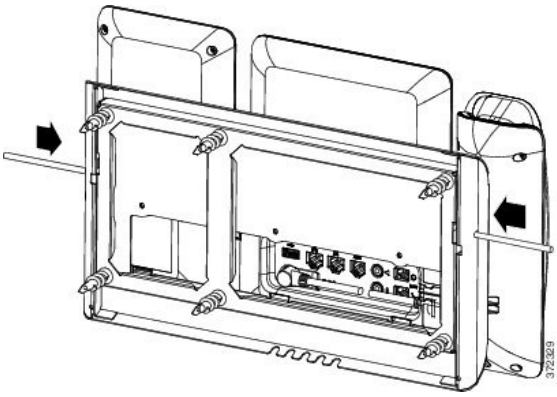
Before You Begin

You require two metal rods.

Procedure

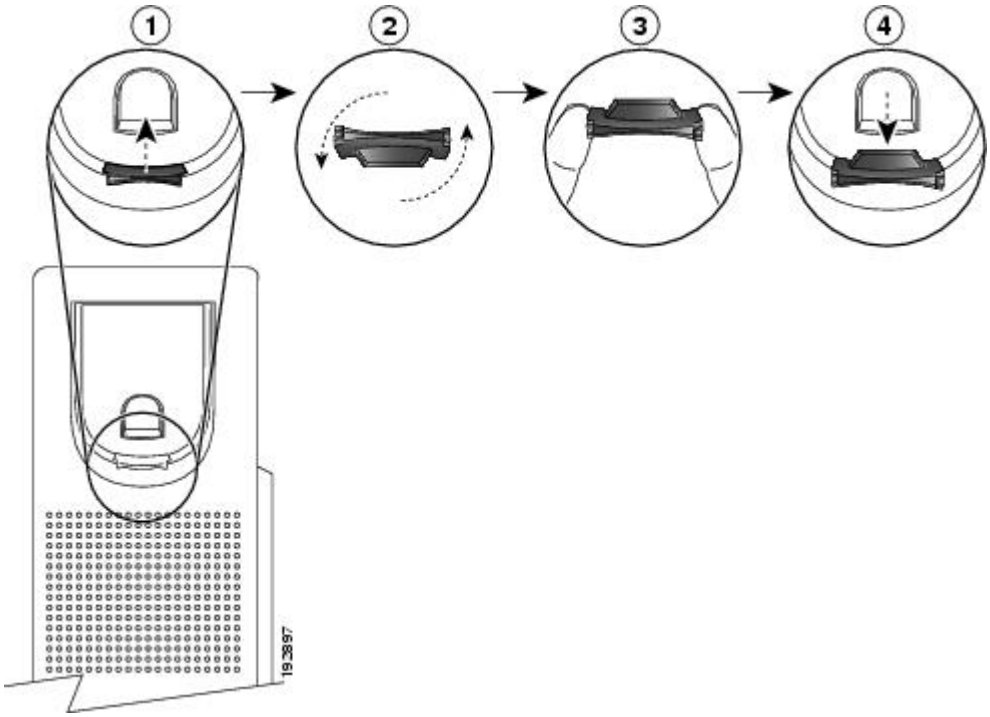
Step 1 Push the rods into the left and right holes in the phone mounting plate approximately 0.75 in (2.0 cm).

Step 2 Press firmly inwards (towards the phone) to disengage the tabs, lift up on the phone to release the phone from the wall bracket, and then pull the phone towards you.



Adjust the Handset Rest

If your phone is wall-mounted, you may need to adjust the handset rest to ensure that the receiver does not slip out of the cradle.



Procedure

Step 1 Remove the handset from the cradle and pull the plastic tab from the handset rest.

Step 2 Rotate the tab 180 degrees.

Step 3 Hold the tab between two fingers, with the corner notches facing you.

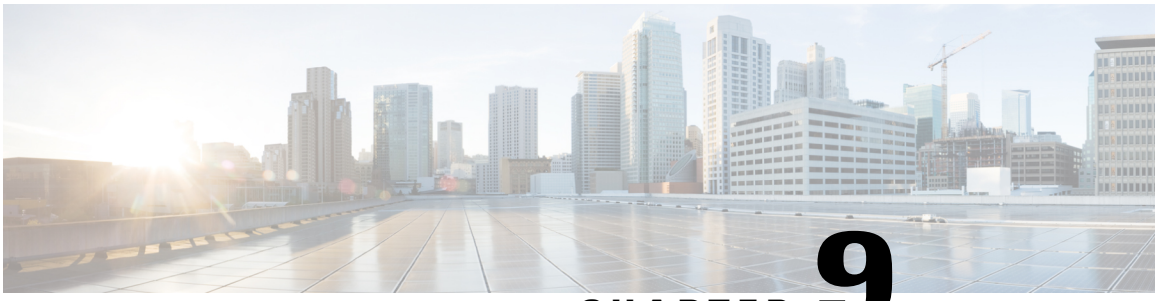
Step 4 Line up the tab with the slot in the cradle and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab.

Step 5 Return the handset to the handset rest.

PART IV

Cisco IP Phone Administration

- Cisco IP Phone Security, page 127
- Cisco IP Phone Customization, page 143
- Phone Features and Setup, page 151
- Corporate and Personal Directory, page 205



CHAPTER 9

Cisco IP Phone Security

- View Current Security Features on Phone, page 127
- View Security Profiles, page 127
- Supported Security Features, page 128

View Current Security Features on Phone

All Cisco IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 Press **Applications**.

Step 2 Choose **Administrator Settings** > **Security Setup**.

View Security Profiles

All Cisco IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

Procedure

Look at the Security Mode setting in the Security Configuration menu.

Supported Security Features

The security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and ensure that the phone uses only digitally signed files.

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for Cisco IP Phones without running the CTL client:

- Signing of the phone configuration files
- Phone configuration file encryption
- HTTPS with Tomcat and other Web services

Note Secure signaling and media features still require you to run the CTL client and use hardware eTokens.

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains secure (encrypted) communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco IP Phones.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the Cisco Unified Communications Manager Security Guide. Alternatively, you can initiate the installation of an LSC from the Security Setup menu on the phone. This menu also lets you update or remove an LSC.

The Cisco IP Phones 8811, 8841, 8851, and 8861 uses the phone security profile, which defines whether the device is nonsecure or secure. For information about applying the security profile to the phone, see the *Cisco Unified Communications Manager Security Guide*.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file contains sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see the "Configuring Encrypted Phone Configuration Files" chapter in the *Cisco Unified Communications Manager Security Guide*.

The following table provides an overview of the security features that the phones support. For more information about these features, Cisco Unified Communications Manager, and Cisco IP Phone security, see the *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, press and choose **Administrator Settings** > **Security Setup**.

Table 15: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering with the firmware image before the image is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Image encryption	Encrypted binary files (with the extension .sebn) prevent tampering with the firmware image before the image is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer site certificate installation	Each Cisco IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify certificate installation in Cisco Unified Communications Manager Administration using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur; and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager does not register phones unless it can authenticate them.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
File encryption	Encryption prevents sensitive information from being revealed while the file is in transit to the phone. In addition, the phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling authentication	Uses the TLS protocol to validate that no tampering to signaling packets has occurred during transmission.
Manufacturing installed certificate	Each Cisco IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC provides permanent unique proof of identity for the phone and allows Cisco Unified Communications Manager to authenticate the phone.
Media encryption	Uses SRTP to ensure that media streams between supported devices prove secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.

Feature	Description
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.
Security profile	Defines whether the phone is nonsecure, authenticated, encrypted, or protected. Other entries in this table describe security features. For more information about these features, about Cisco Unified Communications Manager, and about Cisco IP Phone security, see the *Cisco Unified Communications Manager Security Guide*.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional web server disabling for a phone	For security purposes, you can prevent access to the web pages for a phone (which display a variety of operational statistics for the phone) and Self Care Portal. For more information, see Control Phone Web Page Access, on page 197.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling PC port • Disabling Gratuitous ARP (GARP) • Disabling PC Voice VLAN access • Disabling access to the Setting menus, or providing restricted access that allows access to the Preferences menu and saving volume changes only • Disabling access to web pages for a phone • Disabling Bluetooth Accessory Port
802.1X Authentication	The Cisco IP Phone can use 802.1X authentication to request and gain access to the network. See 802.1X Authentication, on page 139 for more information.
Secure SIP Failover for SRST	After you configure a Survivable Remote Site Telephony (SRST) reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Signaling encryption	Ensures that all SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
Trust List update alarm	When the Trust List updates on the phone, the Cisco Unified Communications Manager receives an alarm to indicate the success or failure of the update. See the following table for more information.

The following table contains the Trust List update alarm messages and meaning. For more information, see the Cisco Unified Communications Manager documentation.

Table 16: Trust List Update Alarm Messages

Code and Message	Description
1 - TL_SUCCESS	Received new CTL and/or ITL
2 - CTL_INITIAL_SUCCESS	Received new CTL, no existing TL
3 - ITL_INITIAL_SUCCESS	Received new ITL, no existing TL
4 - TL_INITIAL_SUCCESS	Received new CTL and ITL, no existing TL
5 - TL_FAILED_OLD_CTL	Update to new CTL failed, but have previous TL
6 - TL_FAILED_NO_TL	Update to new TL failed, and have no old TL
7 - TL_FAILED	Generic failure
8 - TL_FAILED_OLD_ITL	Update to new ITL failed, but have previous TL
9 - TL_FAILED_OLD_TL	Update to new TL failed, but have previous TL

The Security Setup menu provides information about various security settings. The menu also provides access to the Trust List menu and indicates whether the CTL or ITL file is installed on the phone.

The following table describes the options in the Security Setup menu.

Table 17: Security Setup Menu

Option	Description	To change
Security Mode	Displays the security mode that is set for the phone.	From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. The setting appears in the Protocol Specific Information portion of the Phone Configuration window.
LSC	Indicates whether a locally significant certificate that is used for security features is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, see the "Using the Certificate Authority Proxy Function" chapter in the *Cisco Unified Communications Manager Security Guide*.

Option	Description	To change
Trust List	The Trust List provides submenus for the CTL, ITL, and Signed Configuration files. The CTL File submenu displays the contents of the CTL file. The ITL File submenu displays contents of the ITL file. The Trust List menu also displays the following information: • CTL Signature: the SHA1 hash of the CTL file • Unified CM/TFTP Server: the name of the Cisco Unified Communications Manager and TFTP Server that the phone uses. Displays a certificate icon if a certificate is installed for this server. • CAPF Server: the name of the CAPF server that the phone uses. Displays a certificate icon if a certificate is installed for this server. • SRST Router: the IP address of the trusted SRST router that the phone can use. Displays a certificate icon if a certificate is installed for this server.	For more information, see Set Up Locally Significant Certificate, on page 132.
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See 802.1X Authentication, on page 139.

Set Up Locally Significant Certificate

Use this procedure to configure an LSC on the phone.

Before You Begin

Make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL or ITL file has a CAPF certificate.
- In Cisco Unified Communications Operating System Administration, verify that the CAPF certificate is installed.
- The CAPF is running and configured.

For more information about these settings, see the “Configuring the Cisco CTL Client” section in the *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 Obtain the CAPF authentication code that was set when the CAPF was configured.

Step 2 From the phone, press **Applications** and choose **Administrator Settings** > **Security Setup**.

Note You can control access to the Settings menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Step 3 Choose **LSC** and press **Select** or **Update**.
The phone prompts for an authentication string.

Step 4 Enter the authentication code and press **Submit**.
The phone begins to install, update, or remove the LSC, depending on how the CAPF is configured. During the procedure, a series of messages appears in the LSC option field in the Security Configuration menu, so you can monitor progress. When the procedure is complete, Installed or Not Installed displays on the phone.

The LSC install, update, or removal process can take a long time to complete.

When the phone installation procedure is successful, the `Installed` message displays. If the phone displays `Not Installed`, then the authorization string may be incorrect or the phone may not enabled for upgrading. If the CAPF operation deletes the LSC, the phone displays `Not Installed` to indicate that the operation succeeded. The CAPF server logs the error messages. See the CAPF server documentation to locate the logs and to understand the meaning of the error messages.

Phone Call Security

When security is implemented for a phone, you can identify secure phone calls by icons on the phone screen. You can also determine whether the connected phone is secure and protected if a security tone plays at the beginning of the call.

In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security, providing integrity and privacy to the call. When a call in progress is encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to the following icon: .

Note If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

In a secure call, a security tone plays at the beginning of a call to indicate that the other connected phone is also receiving and transmitting secure audio. If your call connects to a nonsecure phone, the security tone does not play.

Note Secure calling is supported for connections between two phones only. Some features, such as conference calling and shared lines, are not available when secure calling is configured.

When a phone is configured as secure (encrypted and trusted) in Cisco Unified Communications Manager, it can be given a "protected" status. After that, if desired, the protected phone can be configured to play an indication tone at the beginning of a call:

- Protected Device: To change the status of a secure phone to protected, check the "Protected Device" check box in the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Phone**).
- Play Secure Indication Tone: To enable the protected phone to play a secure or nonsecure indication tone, set the Play Secure Indication Tone setting to True. By default, Play Secure Indication Tone is set to False. You set this option in Cisco Unified Communications Manager Administration (**System** > **Service Parameters**). Select the server and then the Unified Communications Manager service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. The default is False.

Secure Conference Call Identification

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established by using this process:

1. A user initiates the conference from a secure phone.
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays the secure icon to the right of **Conference** on the phone screen.

Note Secure calling is supported between two phones. Secure conference, Cisco Extension Mobility, and shared lines can be configured by secure conference bridge.

The following table provides information about changes to conference security levels depending on the initiator phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 18: Security Restrictions with Conference Calls

Initiator phone security level	Feature used	Security level of participants	Results of action
Nonsecure	Conference	Secure	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	Secure	Secure conference bridge Secure encrypted level conference

Initiator phone security level	Feature used	Security level of participants	Results of action
Nonsecure	Meet Me	Minimum security level is encrypted.	Initiator receives message `Does not meet Security Level, call rejected`.
Secure	Meet Me	Minimum security level is nonsecure.	Secure conference bridge Conference accepts all calls.

Secure Phone Call Identification

A secure call is established when your phone, and the phone on the other end, is configured for secure calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Secured calls can only be made between two phones. Conference calls should support secure call after secure conference bridge set up.

A secured call is established using this process:

1. A user initiates the call from a secured phone (secured security mode).
2. The phone displays the secure icon on the phone screen. This icon indicates that the phone is configured for secure calls, but this does not mean that the other connected phone is also secured.
3. The user hears a security tone if the call connects to another secured phone, indicating that both ends of the conversation are encrypted and secured. If the call connects to a nonsecure phone, the user does not hear the security tone.

Note Secured calling is supported for conversations between two phones. Some features, such as conference calling and shared lines, are not available when secured calling is configured.

Only protected phones play these secure or nonsecure indication tones. Nonprotected phones never play tones. If the overall call status changes during the call, the indication tone changes and the protected phone plays the appropriate tone.

A protected phone plays a tone or not under these circumstances:

- When the Play Secure Indication Tone option is enabled:
  - When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone (three long beeps with pauses).
  - When end-to-end nonsecure media is established and the call status is nonsecure, the phone plays the nonsecure indication tone (six short beeps with brief pauses).

If the Play Secure Indication Tone option is disabled, no tone plays.

Note Secure calling is supported for connections between two phones only. Some features, such as conference calling and shared lines, are not available when secure calling is configured.

Provide Encryption for Barge

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and security in the system.

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder (fast busy) tone plays on the phone that the barge was initiated.

If the initiator phone is configured for encryption, the barge initiator can barge into a nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

WLAN Security

Because all WLAN devices that are within range can receive all other WLAN traffic, securing voice communications is critical in WLANs. To ensure that intruders do not manipulate nor intercept voice traffic, the Cisco SAFE Security architecture supports the Cisco IP Phone and Cisco Aironet APs. For more information about security in networks, see http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications by using the following authentication methods that the wireless Cisco IP Phone supports:

- Open Authentication: Any wireless device can request authentication in an open system. The AP that receives the request may grant authentication to any requestor or only to requestors that are found on a list of users. Communication between the wireless device and AP could be nonencrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that use WEP only attempt to authenticate with an AP that is using WEP.
- Shared Key Authentication: The AP sends an unencrypted challenge text string to any device that attempts to communicate with the AP. The device that is requesting authentication uses a preconfigured WEP key to encrypt the challenge text and sends it back to the AP. If the challenge text is encrypted correctly, the AP allows the requesting device to authenticate. A device can authenticate only if the device WEP key matches the WEP key on the APs.

  Note Shared Key Authentication is not applicable to Cisco IP Phone 8861.

  Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication: This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server, such as the Cisco Access Control Server (ACS).

  The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with the master key. Both endpoints now contain the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS server.

  Note In the Cisco ACS, by default, the PAC expires in one week. If the phone has an expired PAC, authentication with the RADIUS server takes longer while the phone gets a new PAC. To avoid PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

- Protected Extensible Authentication Protocol (PEAP): Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco IP Phone can use PEAP for authentication with the wireless network.

The following authentication schemes use the RADIUS server to manage authentication keys:

- WPA/WPA2: Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA preshared keys that are stored on the AP and phone.
- Cisco Centralized Key Management (CCKM): Uses RADIUS server and a wireless domain server (WDS) information to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA/WPA2 and CCKM, encryption keys are not entered on the phone, but are automatically derived between the AP and phone. But the EAP username and password that are used for authentication must be entered on each phone.

To ensure that voice traffic is secure, the Cisco IP Phone supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, both the signalling SIP packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the Cisco IP Phone.

WEP

With WEP use in the wireless network, authentication happens at the AP by using open or shared-key authentication. The WEP key that is setup on the phone must match the WEP key that is configured at the AP for successful connections. The Cisco IP Phone supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and AP.

EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the AP after authentication for encrypting all voice packets; consequently, these WEP keys can change with each authentication.

TKIP

WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.

AES

An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, which supports key sizes of 128, 192 and 256 bits, as a minimum. The Cisco IP Phone supports a key size of 256 bits.

Note The Cisco IP Phone does not support Cisco Key Integrity Protocol (CKIP) with CMIC.

Authentication and encryption schemes are set up within the wireless LAN. VLANs are configured in the network and on the APs and specify different combinations of authentication and encryption. An SSID associates with a VLAN and the particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the Cisco IP Phone.

Some authentication schemes require specific types of encryption. With Open authentication, you can use static WEP for encryption for added security. But if you are using Shared Key authentication, you must set static WEP for encryption, and you must configure a WEP key on the phone.

Note

- When you use WPA pre-shared key or WPA2 pre-shared key, the pre-shared key must be statically set on the phone. These keys must match the keys that are on the AP.
- The Cisco IP Phone does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the Cisco IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 19: Authentication and Encryption Schemes

Cisco AP configuration			**Cisco IP Phone configuration**
Authentication	Key management	Common encryption	Authentication
Open		None	Open
Open (Static WEP)		WEP	Open+WEP
Shared key (Static WEP)		WEP	Shared+WEP

Cisco AP configuration			Cisco IP Phone configuration
PEAP 802.1x	Optional CCKM	WEP	PEAP
PEAP WPA	WPA with optional CCKM	TKIP	PEAP
PEAP WPA2	WPA2	AES	PEAP
EAP-FAST 802.1x	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA	WPA Optional CCKM	TKIP	EAP-FAST
EAP-FAST with WPA2	WPA2	AES	EAP-FAST

For additional information about Cisco WLAN Security, see http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html.

For more information about configuring authentication and encryption schemes on APs, see the *Cisco Aironet Configuration Guide* for your model and release under the following URL:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

802.1X Authentication

The Cisco IP Phones support 802.1X Authentication.

Cisco IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations. Cisco IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

Cisco IP Phones also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the IP phone, the LAN switch does not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. Cisco IP Phones contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.

- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the phone must both be configured with a shared secret that authenticates the phone.
- Cisco Catalyst Switch (or other third-party switch): The switch must support 802.1X, so it can act as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure PC Port: The 802.1X standard does not consider VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.
  - Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
  - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.
- Enter MD5 Shared Secret: If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted.

Related Topics

Network Protocols, on page 8

Access 802.1X Authentication

You can access the 802.1X authentication settings by following these steps:

Procedure

Step 1 Press Applications.

Step 2 Choose **Administrator Settings** > **Security Setup** > **802.1X Authentication**.

Step 3 Configure the Options as described in 802.1X Authentication Options, on page 141.

Step 4 To exit this menu, press **Exit**.

802.1X Authentication Options

The following table describes the 802.1X authentication options.

Table 20: 802.1X Authentication Settings

Option	Description	To change
Device Authentication	Determines whether 802.1X authentication is enabled: • Enabled: Phone uses 802.1X authentication to request network access. • Disabled: Default setting. The phone uses CDP to acquire VLAN and network access.	See Set Device Authentication Field, on page 142.
Transaction Status	State: Displays the state of 802.1x authentication: • Disconnected: Indicates that 802.1x authentication is not configured on the phone. • Authenticated: Indicates that the phone is authenticated. • Held: Indicates that the authentication process is in progress. Protocol: Displays the EAP method that is used for 802.1x authentication (can be EAP-FAST or EAP-TLS).	Display only. Cannot configure.

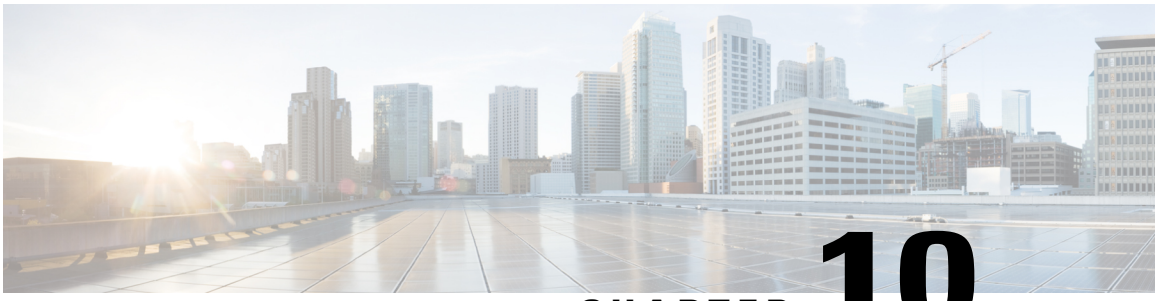
Set Device Authentication Field

Procedure

Step 1 After pressing **Applications** , choose **Administrator Settings** > **Security Setup** > **802.1X Authentication**.

Step 2 Set the Device Authentication option to **Yes** or **No**.

Step 3 Press **Apply**.



CHAPTER 10

Cisco IP Phone Customization

- Custom Phone Rings, page 143
- Custom Background Images, page 145
- Set Up Wideband Codec, page 147
- Set Up Idle Display, page 148

Custom Phone Rings

The Cisco IP Phone ships with three ring tones that are implemented in hardware: Sunshine, Chirp, Chirp1.

Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist-wb.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

Attention All file names are case sensitive. If you use ringlist-wb.xml for the file name, the phone will not apply your changes.

For more information, see the "Cisco TFTP" chapter in *Cisco Unified Communications Manager System Guide* and the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Set Up Custom Phone Rings

To create custom phone rings for the Cisco IP Phone, perform these steps:

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in Custom Ring File Formats, on page 144.

Step 2 Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Step 3 Use a text editor to edit the Ringlist-wb.xml file. See Custom Ring File Formats, on page 144 for information about how to format this file and for a sample Ringlist.xml file.

Step 4 Save your modifications and close the Ringlist-wb.xml file.

Step 5 To cache the new Ringlist-wb.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the "Enable Caching of Constant and Bin Files at Startup" TFTP service parameter, located in the Advanced Service Parameters area.

Custom Ring File Formats

The Ringlist.xml file defines an XML object that contains a list of phone ring types. This file includes up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that appears on the Ring Type menu on a Cisco IP Phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names. You must include the required DisplayName and FileName for each phone ring type.

- DisplayName specifies the name of the custom ring for the associated PCM file that displays on the Ring Type menu of the Cisco IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note The DisplayName and FileName fields must not exceed 25 characters in length.

This example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
```

```
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

The PCM files for the rings must meet the following requirements for proper playback on Cisco IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- Mu-law compression
- Maximum ring size = 16080 samples
- Minimum ring size = 240 samples
- Number of samples in the ring = multiple of 240.
- Ring start and end at zero crossing.

To create PCM files for custom phone rings, use any standard audio editing package that supports these file format requirements.

Custom Background Images

You can provide users with a choice of background images (or wallpaper) for the LCD screen on their phones. Users can select a background image by choosing **Applications** > **Settings** > **Wallpaper** on the phone.

The image choices that users see come from PNG images and an XML file (called List.xml) that are stored on the TFTP server that the phone uses. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

Note The dimensions for the PNG and List.xml images must be within 800x480x24.

Attention All file names are case sensitive. If you use list.xml for the file name, the phone will not apply your changes.

You can disable the option for users to select a background image by unchecking the Enable End User Access to Phone Background Image Setting check box from the Common Phone Profile Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Device Settings** > **Common Phone Profile**). When this check box is unchecked, the **Applications** > **Settings** > **Wallpaper** option does not display on the phone.

Set Up Custom Background Image

To create custom background images for the Cisco IP Phone, follow these steps.

Procedure

Step 1 Create two PNG files for each image (a full-size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in Custom Background File Formats, on page 146.

Step 2 Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:
Desktops/800x480x24

Note The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

To upload the files, choose **Software Upgrades** > **Upload TFTP Server File** in Cisco Unified Communications Operating System Administration. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Note If the folder does not exist, the folder gets created and the files get uploaded to the folder.

Step 3 You must also copy the customized images and files to the other TFTP servers that the phone may contact to obtain these files.

Note Cisco recommends that you store backup copies of custom image files in a different location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 4 Use a text editor to edit the List.xml file. See Custom Background File Formats, on page 146 for the file location, file, formatting requirements, and a sample file.

Step 5 Save your modifications and close the List.xml file.

Note When you upgrade Cisco Unified Communications Manager, a default List.xml file replaces your customized List.xml file. After you customize the List.xml file, make a copy of the file and store it in a different location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 6 To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter that is located in the Advanced Service Parameters area.

Custom Background File Formats

The List.xml file defines an XML object that contains a list of background images. The List.xml file is stored in the following subdirectory on the TFTP server:

Desktops/800x480x24

Tip If you are manually creating the directory structure and the List.xml file, you must ensure that the directories and files can be accessed by the user\CCMService, which is used by the TFTP service.

For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

The List.xml file can include up to 50 background images. The images are in the order that they appear in the Background Images menu on the phone. For each image, the List.xml file contains one element type, called ImageItem. The ImageItem element includes these two attributes:

- Image: Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that appears on the Background Images menu on a phone.
- URL: URI that specifies where the phone obtains the full-size image.

The following example shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image. The TFTP URI that is shown in the example is the only supported method for linking to full-size and thumbnail images. HTTP URL support is not provided.

List.xml Example

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/800x480x24/TN-Fountain.png"
URL="TFTP:Desktops/640x480x24/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/800x480x24/TN-FullMoon.png"
URL="TFTP:Desktops/640x480x24/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

The Cisco IP Phone firmware includes a default background image. The List.xml file does not define this image. The default image is always the first image that appears in the Background Images menu on the phone.

Each background image requires two PNG files:

- Full size image: Version that appears on the on the phone.
- Thumbnail image: Version that displays on the Background Images screen from which users can select an image. Must be 25% of the size of the full-size image.

Tip Many graphics programs provide a feature that resizes a graphic. An easy way to create a thumbnail image is to first create and save the full-size image, then use the sizing feature in the graphics program to create a version of that image that is 25% of the original size. Save the thumbnail version by using a different name.

The PNG files for background images must meet the following requirements for proper display on the Cisco IP Phone:

- Full size image - 800 pixels (width) X 480 pixels (height).
- Thumbnail image - 159 pixels (width) X 109 pixels (height).

Tip If you are using a graphics program that supports a posterize feature for grayscale, set the number of tonal levels per channel to 16, and the image posterizes to 16 shades of grayscale.

Set Up Wideband Codec

By default, the G.722 codec is enabled for the Cisco IP Phone. If Cisco Unified Communications Manager is configured to use G.722 and if the far endpoint supports G.722, the call connects using the G.722 codec in place of G.711.

This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call.

Greater sensitivity means improved audio clarity but also means that the far endpoint can hear more background noise: noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722 distracting. Other users may prefer the additional sensitivity of G.722.

The Advertise G.722 and iSAC Codec service parameter affects whether wideband support exists for all devices that register with this Cisco Unified Communications Manager server or for a specific phone, depending on the Cisco Unified Communications Manager Administration window where the parameter is configured.

Procedure

Step 1 To configure wideband support for all devices:

a) From Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**

b) Set the Advertise G.722 and iSAC Codec field
The default value of this enterprise parameter is **True**, which means that all Cisco IP Phone Models that register to this Cisco Unified Communications Manager advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in the capabilities set, Cisco Unified Communications Manager chooses that codec for the call whenever possible.

Step 2 To configure wideband support for a specific device:

a) From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

b) Set the Advertise G.722 and iSAC Codec parameter in the Product Specific Configuration area.
The default value of this product-specific parameter is to use the value that the enterprise parameter specifies. If you want to override this on a per-phone basis, choose **Enabled** or **Disabled**

Set Up Idle Display

You can specify an idle display (text only; text file size should not exceed 1M bytes) that appears on the phone screen. The idle display is an XML service that the phone invokes when the phone is idle (not in use) for a designated period and no feature menu is open.

For detailed instructions about creating and displaying the idle display, see *Creating Idle URL Graphics on Cisco IP Phone* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

In addition, see the *Cisco Unified Communications Manager Administration Guide* or the *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

- Specifying the URL of the idle display XML service:
  - For a single phone: Idle field in the Phone Configuration window in Cisco Unified Communications Manager Administration.
  - For multiple phones simultaneously: URL Idle field in the Enterprise Parameters Configuration window, or the Idle field in the Bulk Administration Tool (BAT)
- Specifying the length of time that the phone is not used before the idle display XML service is invoked:

- For a single phone: Idle Timer field in the Phone configuration window in Cisco Unified Communications Manager Administration.
- For multiple phones simultaneously: URL Idle Time field in the Enterprise Parameters Configuration window, or the Idle Timer field in the Bulk Administration Tool (BAT)

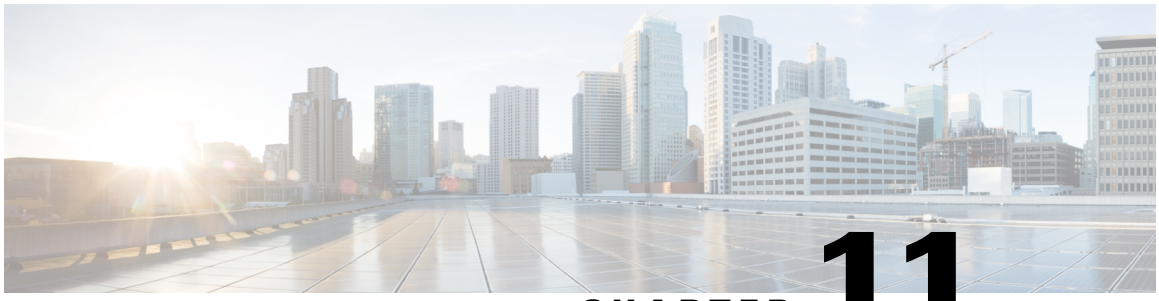
Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**

Step 2 In the Idle field, enter the URL to the idle display XML Service.

Step 3 In the Idle Timer field, enter the time that the idle phone waits before displaying the idle display XML service.

Step 4 Select **Save**.



CHAPTER 11

Phone Features and Setup

- Phone Features and Setup Overview, page 152
- Cisco IP Phone User Support, page 152
- Telephony Features, page 153
- Feature Buttons and Softkeys, page 171
- Disable Speakerphone, page 173
- Schedule Power Save for Cisco IP Phone, page 173
- Schedule Power Save Plus (EnergyWise) on Cisco IP Phone, page 174
- Enable Agent Greeting, page 177
- Set Up the DF Bit, page 178
- Set Up Do Not Disturb, page 178
- Set Up Monitoring and Recording, page 179
- Set Up Power Negotiation for LLDP, page 180
- Set Up Bluetooth Profiles, page 180
- Set Up Automatic Port Synchronization, page 181
- Set Up SSH Access, page 181
- Set Up Call Forward Notification, page 182
- Set Up Client Matter Codes, page 183
- Enable BLF for Call Lists, page 183
- Set Up Dual Bank Information, page 184
- Set Up Forced Authorization Codes, page 184
- Set Up Incoming Call Toast Timer, page 185
- Set Up Peer Firmware Sharing, page 185
- Set Up Remote Port Configuration, page 186
- Set Headset Sidetone Control, page 187

- Enable Device Invoked Recording, page 188
- Set Up Dial Tone from Release Button, page 188
- Park Monitoring, page 189
- Enable Actionable Incoming Call Alert, page 191
- Enable the Call History Display Enhancement, page 192
- Enable Call History for Shared Line, page 193
- Set Up the Default Line Filter, page 193
- Set Up Custom Line Filter, page 193
- Phone Button Templates, page 194
- Control Phone Web Page Access, page 197
- Set Up Softkey Template, page 198
- Set Up RTP/sRTP Port Range, page 200
- Set Up TLS Resumption Timer, page 201
- Set Up Visual Voicemail, page 202
- Enable Intelligent Proximity, page 203
- Manage Join Across Lines and Transfer Across Lines, page 204

Phone Features and Setup Overview

After you install Cisco IP Phones in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use the Cisco Unified Communications Manager Administration application to configure telephony features, optionally modify phone templates, set up services, and assign users.

You can modify additional settings for the Cisco IP Phone from Cisco Unified Communications Manager Administration. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

Related Topics

Cisco IP Phone User Support, on page 152
Cisco Unified Communications Manager Documentation, on page xv
International User Support, on page 269

Cisco IP Phone User Support

If you are a system administrator, you are likely the primary source of information for Cisco IP Phone users in your network or company. It is important to provide current and thorough information to end users.

To successfully use some of the features on the Cisco IP Phone (including Speed Dial, Services, and voice message system options), users must receive information from you or from your network team or must be

able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their Cisco IP Phones.

Consider including the following types of information on this site:

- user guides for all Cisco IP Phone models that you support
- information on how to access the Cisco Unified Communications Self Care Portal
- list of features supported
- user guide or quick reference for your voicemail system

Telephony Features

After you add Cisco IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Cisco Unified Communications Manager Administration.

For information about using most of these features on the phone, see *Cisco IP Phone 8811, 8841, 8851, and 8861 User Guide for Cisco Unified Communications Manager*. See Feature Buttons and Softkeys, on page 171 for a list of features that can be configured as programmable buttons and dedicated softkeys and feature buttons.

Note Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information on accessing and configuring service parameters, see the *Cisco Unified Communications Manager Administration Guide*.

For more information on the functions of a service, select the name of the parameter or the question mark (?) help button in the Service Parameter Configuration window.

Feature	Description and more information
Abbreviated Dialing	Allows users to speed dial a phone number by entering an assigned index code (1-199) on the phone keypad. **Note** You can use Abbreviated Dialing while on-hook or off-hook. Users assign index codes from the Self Care Portal. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone setup" • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone"

Feature	Description and more information
Agent Greeting	Allows an agent to create and update a prerecorded greeting that plays at the beginning of a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple ones as needed. See Enable Agent Greeting, on page 177.
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup Configuration" chapter.
Assisted Directed Call Park	Enables users to park a call by pressing only one button using the Direct Park feature. Administrators must configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button. See the *Cisco Unified Communications Manager Features and Services Guide*, "Assisted Directed Call Park" chapter.
Audible Message Waiting Indicator (AMWI)	A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line. **Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset. See the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.
Automatic Port Synchronization	Synchronizes ports to the lowest speed between ports of a phone to eliminate packet loss. See Set Up Automatic Port Synchronization, on page 181.
Auto Pickup	Allows a user to use one-touch pickup functionality for call pickup features. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Block External to External Transfer	Prevents users from transferring an external call to another external number. See the *Cisco Unified Communications Manager Features and Services Guide*, "External Call Transfer Restrictions" chapter.
Bluetooth Multiconnection	Enables the user to pair multiple devices to the phone. The user can then connect a mobile device using Bluetooth and a Bluetooth headset at the same time.

Feature	Description and more information
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button on the phone. See the *Cisco Unified Communications Manager Features and Services Guide*, "Presence" chapter.
Busy Lamp Field (BLF) Pickup	Provides enhancements to BLF speed dial. Allows you to configure a Directory Number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. See: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Call Back"
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions"
Call Forward	Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. See: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • Customize Self Care Portal Display, on page 80

Feature	Description and more information
Call Forward All Loop Breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.
Call Forward All Loop Prevention	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.
Call Forward Configurable Display	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows. See: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone"
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external. See the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers" chapter.
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call. See Set Up Call Forward Notification, on page 182.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature will: • Log missed calls for a shared line • Log all answered and placed calls for a shared line See Enable Call History for Shared Line, on page 193
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter.

Feature	Description and more information
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Call Recording	Allows a supervisor to record an active call. The user might hear a recording audible alert tone during a call when it is being recorded. When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being recorded. **Note** When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call. See the *Cisco Unified Communications Manager Features and Services Guide*, "Monitoring and Recording" chapter.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display. See the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers".
Call Waiting Ring	Provides Call Waiting users with the option of an audible ring instead of the standard beep. Options are Ring and Ring Once. See the *Cisco Unified Communications Manager System Guide*, "Directory Numbers".
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration".

Feature	Description and more information
Caller ID Blocking	Allows a user to block their phone number or email address from phones that have caller identification enabled. See: • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration"
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book. See the *Cisco Unified Communications Manager Features and Services Guide*, "Calling Party Normalization" chapter.
CAST for SIP	Establishes communication between the Cisco Unified Video Advantage (CUVA) and the Cisco IP phones to support video on the PC even if the IP phone does not have video capability. See the *Cisco Unified Communications Manager Features and Services Guide*.
cBarge	Allows a user to join a nonprivate call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. The conference call is created using the Cisco Unified Communications Manager conference bridge functionality. In Firmware Release 10.2(2) and later, the cBarge functionality is accessed using the Merge softkey. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy"
Charge a Mobile Device	Allows a user to charge a mobile device by connecting it to the USB port of the Cisco IP Phone. See *Cisco IP Phone 8841, 8851, and 8861 User Guide for Cisco Unified Communications Manager* .

Feature	Description and more information
Cisco Extension Mobility	Allows users to temporarily access their Cisco IP Phone configuration such as line appearances, services, and speed dials from shared Cisco IP Phone by logging into the Cisco Extension Mobility service on that phone when they log into the Cisco Extension Mobility service on that phone. Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers. See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Extension Mobility" chapter.
Cisco Extension Mobility Cross Cluster (EMCC)	Enables a user configured in one cluster to log into a Cisco IP Phone in another cluster. Users from a home cluster log into a Cisco IP Phone at a visiting cluster. **Note** Configure Cisco Extension Mobility on Cisco IP Phones before you configure EMCC. See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Extension Mobility Cross Cluster" chapter.
Cisco IP Phone 8800 Key Expansion Module	Provides additional keys by adding an expansion module to the phone. See Cisco IP Phone Key Expansion Module, on page 93.
Cisco IP Phone 8811 Support	Provides support for the Cisco IP Phone 8811.
Cisco Unified Communications Manager Express (Unified CME) Version Negotiation	The Cisco Unified Communication Manager Express uses a special tag in the information sent to the phone to identify itself. This tag enables the phone to provide services to the user that the switch supports. See: • *Cisco Unified Communications Manager Express System Administrator Guide* • Cisco Unified Communications Manager Express Interaction, on page 14
Cisco Unified Video Advantage (CUVA)	Allows users to make video calls by using a Cisco IP Phone, a personal computer, and an external video camera. **Note** Configure the Video Capabilities parameter in the Product Specific Configuration Layout section in Phone Configuration. See the Cisco Unified Video Advantage documentation.
Cisco WebDialer	Allows users to make calls from web and desktop applications. See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco WebDialer" chapter.
Classic Ringtone	Supports ringtones that are embedded in the phone firmware or downloaded from the Cisco Unified Communications Manager. The feature makes the available ringtones common with other Cisco IP Phones. See Custom Phone Rings, on page 143.

Feature	Description and more information
Client Matter Code (CMC)	Enables a user to specify that a call relates to a specific client matter. See Set Up Client Matter Codes, on page 183.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me. Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line. The Advance Adhoc Conference service parameter, disabled by default in Cisco Unified Communications Manager Administration, allows you to enable these features. See the *Cisco Unified Communications Manager System Guide*,"Conference Bridges" and "Cisco Unified IP Phone" chapters. **Note** Be sure to inform your users whether these features are activated.
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection. See the *Cisco Unified Communications Manager Administration Guide*, "CTI Route Point Configuration" chapter.
Decline All	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is declined, the line becomes available to make or receive new calls. See the *Cisco Unified Communications Manager Features and Services Guide*, "Immediate Divert" chapter.
Device Invoked Recording	Provides end users with the ability to record their telephone calls via a softkey. In addition administrators may continue to record telephone calls via the CTI User Interface. See Enable Device Invoked Recording, on page 188.
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter.
Display Battery Strength and Signal Strength Icons	Displays the battery and signal strength of the mobile phone on the IP Phone when the mobile phone is connected to the IP Phone using Bluetooth.

Feature	Description and more information
Distinctive Ring	Users can customize how their phone indicates an incoming call and a new voice mail message. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. See Set Up Do Not Disturb, on page 178.
Enable/Disable JAL/TAL	Allows the administrator to control the Join Across Lines (JAL) and Direct Transfer Across Lines (TAL) features. See Manage Join Across Lines and Transfer Across Lines, on page 204.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings. See Schedule Power Save Plus (EnergyWise) on Cisco IP Phone, on page 174.
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC). See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Extension Mobility Cross Cluster" chapter.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. See "Services" in this table. See Modify Phone Button Template for PAB or Fast Dial, on page 196.
Forced Authorization Code (FAC)	Controls the types of calls that certain users can place. See Set Up Forced Authorization Codes, on page 184.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset. See Set Headset Sidetone Control, on page 187.

Feature	Description and more information
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble. You can configure call focus priority to favor incoming or reverting calls. See the *Cisco Unified Communications Manager Features and Services Guide*, "Hold Reversion" chapter.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. • No configuration required unless you want to use Music On Hold. See "Music On Hold" in this table for information. • See "Hold Reversion" in this table.
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.
Hunt Group	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone. See: • *Cisco Communications Manager Administration Guide*, "Hunt Group Configuration" • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"
Incoming Call Toast Timer	Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen. See Set Up Incoming Call Toast Timer, on page 185.
Intelligent Proximity	Enables users to pair a mobile device with the phone using Bluetooth and use the phone to place and receive mobile calls, See Enable Intelligent Proximity, on page 203.

Feature	Description and more information
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line. See the *Cisco Unified Communications Manager Feature and Services Guide*, "Intercom" chapter.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for audio streams.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on the call.
Line Status for Call Lists	Allows the user to see the Line Status availability status of monitored line numbers in the Call History list. The Line Status states are • Offline • Available • In use • Do not disturb See Enable BLF for Call Lists, on page 183.
Line Status in Corporate Directory	Enables the display of the status of a contact in the Corporate Directory. • Offline • Available • In use • Do not disturb See Enable BLF for Call Lists, on page 183.
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent nonhunt group calls from ringing their phone. See *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"

Feature	Description and more information
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received. See: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide*, "Malicious Call Identification"
Meet Me Conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time. See the *Cisco Unified Communications Manager Administration Guide*, "Meet Me Number/Pattern Configuration" chapter.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco IP Phone. See: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager"
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages. See: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager"
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone.
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance. See the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day. See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter.

Feature	Description and more information
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a cellular phone. See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter.
Monitoring and Recording	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored. When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being monitored. **Note** When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user place an intercom call, the active call will be put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call. See the *Cisco Unified Communications Manager Features and Services Guide*, "Monitoring and Recording" chapter.
Multiple Calls Per Line Appearance	Each line can support multiple calls. By default, the phone supports two active calls per line, and a maximum of six active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold. The system allows you to configure maximum calls/busy trigger not more than 6/6. Any configuration more than 6/6 is not officially supported. See the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.
Music On Hold	Plays music while callers are on hold. See the *Cisco Unified Communications Manager Features and Services Guide*, "Music On Hold" chapter.
Mute	Mutes the handset or headset microphone.
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.
Other Group Pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.

Feature	Description and more information
Phone Display Message for Extension Mobility Users	This feature enhances the phone interface for the Extension Mobility user by providing friendly messages.
Phone Trust List Notification in Cisco Unified Communications Manager	Enables the phone to send an alarm to the Cisco Unified Communications Manager when the Trust List (TL) is updated. See Supported Security Features, on page 128.
PLK Support for Queue Statistics	The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a plus (+) sign. To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call.
Power Negotiation over LLDP	Allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP). See Set Up Power Negotiation for LLDP, on page 180.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone display about the call of the other user. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter
Private Line Automated Ringdown (PLAR)	The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco IP Phone dials as soon as the handset goes off hook. This can be useful for phones that are designated for calling emergency or "hotline" numbers. See the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.
Programmable Feature Buttons	You can assign features, such as New Call, Call Back, and Forward All to line buttons. See: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter

Feature	Description and more information
Quality Reporting Tool (QRT)	Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT. See: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Quality Report Tool" chapter
Redial	Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.
Remote Port Configuration	Allows you to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager Administration. This enhances the performance for large deployments with specific port settings. **Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone. See Set Up Remote Port Configuration, on page 186.
Reroute Direct Calls to Remote Destination to Enterprise Number	Reroutes a direct call to a user's mobile phone to the enterprise number (desk phone). For an incoming call to remote destination (mobile phone), only remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their mobile phone. See the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter.
Remove 'Call Ended' Prompt Timer	Improves the End Call response time by removing the `Call ended` message display on the phone screen.
Ringtone Setting	Identifies ring type used for a line when a phone has another active call. See: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter • Custom Phone Rings, on page 143
RTCP Hold For SIP	Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.

Feature	Description and more information
Secure Conference	Allows secure phones to place conference calls using a secured conference bridge. As new participants are added by using Confrn, Join, or Merge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones. The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set. See: • Supported Security Features, on page 128 • *Cisco Unified Communications Manager System Guide*, "Conference Bridges" chapter • *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Configuration" chapter • *Cisco Unified Communications Manager Security Guide*
Secure EMCC	Improves the EMCC feature by providing enhanced security for a user logging into their phone from a remote office.
Services	Allows you to use the Cisco IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone Services" chapter
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone Services" chapter

Feature	Description and more information
Show Calling ID and Calling Number	The phones can display both the calling ID and calling number for incoming calls. The IP phone LCD display size limits the length of the calling ID and the calling number that display. The Show Calling ID and Calling Number feature applies to the incoming call alert only and does not change the function of the Call Forward and Hunt Group features. See “Caller ID” in this table.
Simplified Tablet Support	Enables an Android or iOS tablet user to pair the tablet to the phone using Bluetooth and then use the phone for the audio part of a call on the tablet. See Enable Intelligent Proximity, on page 203.
Speed Dial	Dials a specified number that has been previously stored. See: • *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” • *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone”
SSH Access	Allows you to enable or disable the SSH Access setting using Cisco Unified Communications Manager Administration. Enabling the SSH server allows the phone to accept the SSH connections. Disabling the SSH server functionality of the phone blocks the SSH access to the phone. See Set Up SSH Access, on page 181.
Time-of-Day Routing	Restricts access to specified telephony features by time period. See: • *Cisco Unified Communications Manager Administration Guide*, “Time Period Configuration” • *Cisco Unified Communications Manager System Guide*, “Time-of-Day Routing”
Time Zone Update	Updates the Cisco IP Phone with time zone changes. See the *Cisco Unified Communications Manager Administration Guide*, “Date/Time Group Configuration” chapter.
Transfer	Allows users to redirect connected calls from their phones to another number.

Feature	Description and more information
Transfer - Direct Transfer	Transfer: The first invocation of Transfer will always initiate a new call by using the same directory number, after putting the active call on hold. The user can directly transfer calls using Transfer Active Call Function. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. See *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers"
TVS	Trust Verification Services (TVS) enables phones to authenticate signed configurations and authenticate other servers or peers without increasing the size of the Certificate Trust List (CTL) or requiring the downloading of an updated CTL file to the phone. TVS is enabled by default. The Security Setting menu on the phone displays the TVS information.
UCR 2013	The Cisco IP Phones support Unified Capabilities Requirements (UCR) 2013 by providing the following functions: • Support for Federal Information Processing Standard (FIPS) 140-2 • Support for 80-bit SRTCP Tagging As an IP Phone administrator, you must set up specific parameters in Cisco Unified Communications Manager Administration.
Unconfigured Primary Line Notification	Alerts the user when the primary line is not configured. The user sees the message `Unprovisioned` on the phone screen.
User Interface Updates for List, Alert, and Visual Voicemail.	Increases the size of the application window to minimize truncated strings.
Visual Voicemail	Replaces the voicemail audio prompts with a graphical interface. See *Installation and Configuration Guide for Visual Voicemail* located at http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3.
Voice Message System	Enables callers to leave messages if calls are unanswered. See: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Voice-Mail Port Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter. • Set Up Visual Voicemail, on page 202

Feature	Description and more information
Web Access Disabled by Default	Enhances security by disabling access to all web services, such as HTTP. Users can only access web services if you enable web access.

Feature Buttons and Softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. An "X" in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco IP Phone administration.

For information about configuring programmable feature buttons, see Phone Button Templates, on page 194.

Table 21: Features and Corresponding Buttons and Softkeys

Feature name	Dedicated feature button	Programmable feature button	Softkey
Alert Calls		X	
All Calls		X	
Answer		X	X
Barge			X (Displays as Merge)
Call Back		X	X
Call Forward All			X
Call Park		X	X
Call Park Line Status		X	
Call Pickup (Pick Up)		X	X
Call Pickup Line Status		X	
Conference	X		X
Divert			X
Do Not Disturb		X	X

Feature name	Dedicated feature button	Programmable feature button	Softkey
Group Pickup (Group Pick Up)		X	X
Hold	X		X
Hunt Groups		X	
Intercom		X	
Malicious Call Identification (MCID)		X	X
Meet Me		X	X
Mobile Connect (Mobility)		X	X
Mute	X		
Other Pickup		X	X
PLK Support for Queue Status			X
Privacy		X	
Queue Status		X	
Quality Reporting Tool (QRT)		X	X
Record			X
Redial		X	X
Speed Dial		X	X
Speed Dial Line Status		X	X
Support for Hold Button on USB Headsets			X
Transfer	X		X

Disable Speakerphone

By default, the speakerphone is enabled on the Cisco IP Phone.

You can disable the speakerphone by using Cisco Unified Communications Manager Administration. When the speakerphone is disabled, the Redial, New Call, and Forward All softkeys are not displayed on the phones when the user presses the speakerphone button. The softkey labels are dimmed or removed.

Procedure

Step 1 Select **Device** > **Phone**.

Step 2 Select the phone you want to modify.

Step 3 In the Phone Configuration window for the phone, check the **Disable Speakerphone** check box.

Step 4 Select **Save**.

Schedule Power Save for Cisco IP Phone

To conserve power and ensure the longevity of the phone screen display, you can set the display to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.

  The phone takes the action designated by that button in addition to turning on the display.
- Lift the handset.

When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the following fields.

Table 22: PowerSave Configuration Fields

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field. Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the display on at 07:00 a.m., (0700), enter **07:00**. To turn the display on at 02:00 p.m. (1400), enter **14:00**. If this field is blank, the display will automatically turn on at 0:00.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field. Enter the value in this field in the format *hours:minutes*. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter **04:30**. If this field is blank, the phone will turn off at the end of the day (0:00). **Note** If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). Enter the value in this field in the format *hours:minutes*. For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after a user turns the display on, enter **01:30**. The default value is 01:00.

Step 4 Select **Save**.

Schedule Power Save Plus (EnergyWise) on Cisco IP Phone

To reduce power consumption, configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller.

You configure settings in Cisco Unified Communications Manager Administration to enable EnergyWise and configure sleep and wake times. These parameters are closely tied to the phone display configuration parameters.

When EnergyWise is enabled and a sleep time is set, the phone sends a request to the switch to wake it up at the configured time. The switch returns either an acceptance or a rejection of the request. If the switch rejects the request or if the switch does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, thus reducing the power consumption to a predetermined level. A phone that is not idle sets an idle timer and goes to sleep after the idle timer expires.

To wake up the phone, press Select. At the scheduled wake time, the system restores power to the phone, waking it up.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the following fields.

Table 23: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.
Phone On Time	Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20.

Field	Description
Phone Off Time	The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.
Phone Off Idle Timeout	The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the **Select** key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is: • At 10 minutes before power down, play the ringtone four times. • At 7 minutes before power down, play the ringtone four times. • At 4 minutes before power down, play the ringtone four times. • At 30 seconds before power down, play the ringtone 15 times or until the phone powers off. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length of this field is 127 characters.

Field	Description
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Step 4 Select **Save**.

Enable Agent Greeting

The Agent Greeting feature allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple greetings, as needed, and create and update the greetings.

When a customer calls, the agent and the caller hear the prerecorded greeting. The agent can remain on mute until the greeting ends or the agent can answer the call over the greeting.

All codecs supported for the phone are supported for Agent Greeting calls.

For more information, see:

- *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter
- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter

Procedure

Step 1 Select **Device** > **Phone**.

Step 2 Locate the IP phone that you want to configure.

Step 3 Scroll to the Device Information Layout pane and set **Built In Bridge** to On or Default.

Step 4 Select **Save**.

Step 5 Check the setting of the bridge:

a) Choose **System** > **Service Parameters**.

b) Select the appropriate Server and Service.

c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.

d) Select **Save**.

Set Up the DF Bit

The Configurable DF Bit feature controls how network packets are sent. Packets can be sent in chunks (fragments) of various sizes. When the DF bit is set to 1 in the packet header, the network payload does not fragment when going through network devices, such as switches and routers. Removing fragmenting avoids incorrect parsing on the receiving side, but results in slightly slower speeds. By default, the DF bit is set to 0.

The DF bit setting does not apply to ICMP, VPN, VXC VPN, or DHCP traffic.

Procedure

Step 1 In the Cisco Unified Communications Manager Administration, navigate to one of the following windows:

- **System** > **Enterprise Phone**
- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone**

Step 2 Set the DF Bit field.

Set Up Do Not Disturb

When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.

You can configure the phone with a phone-button template with DND as one of the selected features.

For more information, see “Do Not Disturb” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Procedure

Step 1 Using Cisco Unified Communications Manager Administration, select **Device** > **Phone**

Step 2 Locate the phone to be configured.

Step 3 Set the following parameters.

- Do Not Disturb: This check box allows you to enable DND on the phone.
- DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.

  Note This parameter is located on both the Common Phone Profile window and the Phone configuration window. The Phone configuration window value takes precedence.

- DND Option: Ring Off, Call Reject, or Use Common Phone Profile Setting.

Step 4 Select **Save**.

Set Up Monitoring and Recording

The Monitoring and Recording feature allows a supervisor to monitor an active call silently. Neither party on the call can hear the supervisor. The user may receive an audible alert during a call when it is being monitored.

When a call is secure, a lock icon displays. Callers may also receive an audible alert to indicate that the call is being monitored. The connected parties may also receive an audible alert that indicates that the call is secure and is being monitored.

When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold. This action causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the person being monitored must resume the call.

For more information, see the "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

The following procedure adds a user to the standard monitoring user groups.

Before You Begin

The Cisco Unified Communications Manager must be configured to support Monitoring and Recording.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **User Management** > **Application User**.

Step 2 Check the Standard CTI Allow Call Monitoring user group and the Standard CTI Allow Call Recording user groups.

Step 3 Click **Add Selected**.

Step 4 Click **Add to User Group**.

Step 5 Add the user phones to the list of Application Users controlled devices.

Step 6 Select **Save**.

Set Up Power Negotiation for LLDP

The Power Negotiation for LLDP feature allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).

Power Negotiation should not be disabled when the phone is connected to a switch that supports power negotiation. If disabled, the switch could shut off power to the phone.

The Power Negotiation feature is enabled by default.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone that you need to set up.

Step 3 In the Product Specific Configuration area, set the Power Negotiation parameter.

Step 4 Select **Save**.

Set Up Bluetooth Profiles

For more information on Bluetooth profiles, see the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones that display in Cisco Unified Communications Manager.

Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.

Step 4 Go to the Product Specific Configuration Layout area and from the Bluetooth Profiles drop-down list, choose the applicable profile.

The Handsfree profile is selected by default.

Step 5 Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.

- If you do not check this check box, the corresponding parameter setting does not take effect.
- Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you also set these same parameters in these other windows, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings (highest precedence)

2 Common Phone Profile Configuration window settings

3 Enterprise Phone Configuration window settings (lowest precedence)

Set Up Automatic Port Synchronization

You can set up synchronization on a single phone or a group of phones.

Procedure

Step 1 To configure Automatic Port Synchronization for a single phone,

a) In the Cisco Unified Communications Manager Administration application, choose **Device** > **Phone**
b) Locate the phone.
c) In the Product Specific Configuration Layout pane, set the Automatic Port Synchronization parameter.
d) Select **Save**.

Step 2 To configure Automatic Port Synchronization for a group of phones,

a) In the Cisco Unified Communications Manager Administration application, choose **System** > **Enterprise Phone Configuration**.
b) Set the Automatic Port Synchronization parameter.
c) Select **Save**.

Set Up SSH Access

You can enable or disable access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks. By default, the SSH daemon is disabled.

The SSH Access parameter is disabled by default. You must enable the SSH Access parameter before users of these phones can use SSH.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose one of the following windows:

- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone** > **Phone Configuration**

Note If you set the parameter in both windows, the setting in the **Device** > **Phone** > **Phone Configuration** window takes precedence.

Step 2 Select the appropriate phones.

Step 3 Scroll to the Product Specific Configuration Layout pane and select **Enable** from the SSH Access drop-down list box.

Step 4 Select **Save**.

Set Up Call Forward Notification

You can control the call forward settings.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone to be set up.

Step 3 Configure the Call Forward Notification fields.

Table 24: Call Forward Notification fields

Field	Description
Caller Name	When this check box is checked, the caller name displays in the notification window. By default, this check box is checked.
Caller Number	When this check box is checked, the caller number displays in the notification window. By default, this check box is not checked.
Redirected Number	When this check box is checked, the information about the caller who last forwarded the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, the notification box that D sees contains the phone information for caller C. By default, this check box is not checked.

Field	Description
Dialed Number	When this check box is checked, the information about the original recipient of the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, then the notification box that D sees contains the phone information for caller B. By default, this check box is checked.

Step 4 Select **Save**.

Set Up Client Matter Codes

You can force users to enter a Client Matter Code (CMC) when placing a call. For more information, see the "Client Matter Codes and Forced Authorization Codes" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Call Routing** > **Client Matter Codes**.

Step 2 Configure the Require Client Matter Code field.
This check box controls whether the system prompts the user for a CMC upon placing a call.

Step 3 Select **Save**.

Enable BLF for Call Lists

The BLF for Call Lists field also controls the Line Status for Corporate Directory feature.

Procedure

Step 1 In the Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.

Step 2 For the BLF for Call Lists field, enable or disable the feature.
By default, the feature is disabled.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings

2 Common Phone Profile window settings

3 Enterprise Phone Configuration window settings

Step 3 Select **Save**.

Set Up Dual Bank Information

To set up Dual Bank Information, follow these steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Defaults**.

Step 2 Check the load information in the Inactive Load Information field.

Step 3 Choose **Bulk Administration** > **Import/Export** > **Export** > **Device Defaults**, and schedule an export job.

Step 4 Download the exported tar file and untar it.

Step 5 Check the file format in the exported CSV file and verify that the CSV file has an Inactive Load Information column with the correct value.

Note The CSV file value must match the Device Default value in the Cisco Unified Communications Manager Administration window.

Set Up Forced Authorization Codes

You can force users to enter a Forced Authorization Code (FAC) when placing a call. For more information, see the "Client Matter Codes and Forced Authorization Codes" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Call Routing** > **Forced Authorization Code**.

Step 2 Configure the following fields.

Field	Description
Require Forced Authorization Code	Select the check box to require a user to enter an FAC.
Authorization Level	The code that the user must enter to be authorized to place the call.

Step 3 Select **Save**.

Set Up Incoming Call Toast Timer

You can set the time that the Incoming Call Toast (incoming call notification window) displays on the user phone.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select one of the following windows:

- **Device** > **Phone**
- **Device** > **Device Settings** > **Common Phone Profile**
- **System** > **Enterprise Phone**

If you configure the parameter in multiple windows, the precedence order is:

1 **Device** > **Phone**

2 **Device** > **Device Settings** > **Common Phone Profile**

3 **System** > **Enterprise Phone**

Step 2 If required, locate the phone.

Step 3 Set the Incoming Call Toast Timer field.

Field	Description
Incoming Call Toast Timer	Gives the time, in seconds, that the toast displays. The time includes the fade-in and fade-out times for the window. The possible values are 0, 3, 4, and 5. 0 denotes disable incoming call toast.

Step 4 Select **Save**.

Set Up Peer Firmware Sharing

When enabled, the feature allows the phone to discover like phones on the subnet that are requesting the files that make the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in the hierarchy, and the files are then rapidly transferred down the transfer hierarchy to the other phones on the subnet that are using TCP connections.

The feature provides the following advantages in high-speed campus LAN settings:

- Limits congestion on TFTP transfers to centralized remove TFTP servers
- Eliminates the need to manually control firmware upgrades
- Reduces phone downtime during upgrades when laree numbers of phones are reset simultaneously

Peer Firmware Sharing may also aid in firmware upgrades in branch or remote office deployment scenarios that run over bandwidth-limited WAN links.

This menu option indicates whether the phone supports peer firmware sharing. Settings include:

- Enabled, which is the default value.
- Disabled

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones that associate with the Cisco Unified Communications Manager.

Step 3 Click on the Device Name of the phone.

Step 4 Go to Product Specific Configuration Layout area and select **Enable** from the Peer Firmware Sharing drop-down list.
The Peer Firmware Sharing is enabled by default.

Step 5 Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.

- If you do not check this check box, the corresponding parameter setting does not take effect.
- Parameters that you set in the Product Specific Configuration area may also appear in the Phone Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order:

1. Device Configuration window settings (highest precedence)
2. Common Phone Profile window settings
3. Enterprise Phone Configuration window settings (lowest precedence)

Step 6 Select **Save**.

Set Up Remote Port Configuration

To configure the Switch Remote Port Configuration parameter or the PC Remote Port Configuration parameter, you can configure individual phones or multiple phones.

Procedure

Step 1 To configure the parameter for individual phones, perform the following steps:

a) In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.
b) Select the appropriate IP phones.
c) Scroll to the Product Specific Configuration Layout area (Switch Port Remote Configuration or PC Port Remote Configuration) and set the parameter.
d) Select **Save**.

Step 2 To configure the setting on multiple phones simultaneously, perform the following steps:

a) In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Phone Configuration**.
b) Configure the Remote Port Configuration parameter.
c) Select **Save**.

Set Headset Sidetone Control

When users handle calls using headsets, they may find that they are hearing feedback as they speak. This additional audio is called sidetone. If there is too much sidetone, users can hear what they are saying in the earpiece of the headset and find this sidetone distracting. The amount of sidetone varies from headset to headset.

You can adjust the sidetone level. Available sidetone levels are:

- High
- Normal (Default)
- Low
- Off

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones.

Step 3 Click on the Device Name of the phone.

Step 4 Go to Product Specific Configuration Layout area and from the Wideband Headset UI Control drop-down list box, choose the applicable profile.
The Off option is selected by default (should be enabled only if the user headset supports wideband).

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings
2 Common Phone Profile window settings
3 Enterprise Phone Configuration window settings

Step 5 Select **Save**.

Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager Administration. For more information and detailed instructions, see the "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Procedure

Step 1 Set the IP phone Built In Bridge to **On**.
Step 2 Set Recording Option to **Selective Call Recording Enabled**.
Step 3 Select the appropriate Recording Profile.

Set Up Dial Tone from Release Button

You can provide users with one-button access to the dial tone and the New Call window from an active call.

The following table describes the field for the Dial Tone from Release button feature.

Field	Description
Provide Dial Tone from Release Key	Identifies if pressing the Release key causes the user to hear dial tone (Enabled) or not (Disabled). The possible values are Disabled or Enabled. The default is Disabled

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to one of the following windows:

- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone** > **Phone Configuration**

Step 2 Set the Provide Dial Tone from Release Key field.

Park Monitoring

Park monitoring is supported only when a Cisco IP Phone 8841, 8851, and 8861 parks a call. Park monitoring then monitors the status of a parked call. The park monitoring call bubble does not clear until the parked call gets retrieved or is abandoned by the parked call. This parked call can be retrieved by using the same call bubble on the phone that parked the call.

Set Up Park Monitoring Timers

Cisco Unified Communications Manager Administration provides three cluster-wide service timer parameters for park monitoring: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer. Each service parameter includes a default and requires no special configuration. These timer parameters are for park monitoring only; the Call Park Display Timer and Call Park Reversion Timer are not used for park monitoring. See the following table for descriptions of these parameters.

Configure the timers in the Cisco Unified Communications Manager Service Parameters page.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 Update the Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer fields in the Clusterwide Parameters (Feature-General) pane.

Table 25: Service Parameters for Park Monitoring

Field	Description
Park Monitoring Reversion Timer	Default is 60 seconds. This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses Park on the phone, and a reminder is issued when the timer expires. You can override the value that this service parameter specifies on a per-line basis in the Park Monitoring section of the Directory Number Configuration window (in Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**). Specify a value of 0 to immediately utilize the periodic reversion interval that the Park Monitoring Periodic Reversion Timer service parameter specifies. (See the description that follows.) For example, if this parameter is set to zero and the Park Monitoring Periodic Reversion Timer is set to 15, the user is immediately prompted about the parked call and every 15 seconds thereafter until the Park Monitoring Forward No Retrieve Timer (see the description that follows) expires.

Field	Description
Park Monitoring Periodic Reversion Timer	Default is 30 seconds. This parameter determines the interval (in seconds) that Cisco Unified Communications Manager waits before prompting the user again that a call is parked. To connect to the parked call, the user can simply go off-hook during one of these prompts. Cisco Unified Communications Manager continues to prompt the user about the parked call as long as the call remains parked and until the time that the Park Monitoring Forward No Retrieve Timer (see the description that follows) specifies expires. Specify a value of 0 to disable periodic prompts about the parked call.
Park Monitoring Forward No Retrieve Timer	Default is 300 seconds. This parameter determines the number of seconds that park reminder notifications occur before the parked call forwards to the Park Monitoring Forward No Retrieve destination that is specified in the parker Directory Number Configuration window. (If no forward destination is provided in Cisco Unified Communications Manager Administration, the call returns to the line that parked the call.) This parameter starts when the time that the Park Monitoring Reversion Timer service parameter specifies expires. When the Park Monitoring Forward No Retrieve Timer expires, the call is removed from park and forwards to the specified destination or returns to the parker line.

Set Park Monitoring Parameters for Directory Numbers

The Directory Number Configuration window contains a Park Monitoring area where you can configure the three parameters.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**.

Step 2 Set the park monitoring fields as described in the following table.

Table 26: Park Monitoring Parameters

Field	Description
Park Monitoring Forward No Retrieve Destination External	When the parkee is an external party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination External parameter. If the Forward No Retrieve Destination External field value is empty, the parkee is redirected to the parker line.
Park Monitoring Forward No Retrieve Destination Internal	When the parkee is an internal party, the call forwards to the specified destination in the parker's Park Monitoring Forward No Retrieve Destination Internal parameter. If the Forward No Retrieve Destination Internal is empty, the parkee is redirected to the parker line.

Field	Description
Park Monitoring Reversion Timer	This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses Park on the phone, and a reminder is issued when the timer expires. Default: 60 seconds If you configure a nonzero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window is used.

Set Up Park Monitoring for Hunt Lists

When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) when the Park Monitoring Forward No Retrieve Timer expires.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

Step 2 Set the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter.
If the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is blank, the call forwards to the destination that is configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires.

Enable Actionable Incoming Call Alert

When this feature is enabled, an actionable alert displays when there is an incoming call. The alert replaces the traditional incoming call pop-up notification, and the user must respond to the alert.

Note If both the Custom Line Filters and Actionable Incoming Call Alert features are enabled, actionable call alerts apply only to the lines that are covered by filters.

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose one of the following:

- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone**

Step 2 Locate the Actionable Incoming Call Alert field and set the field to the appropriate setting.
The possible field values are:

- Disabled: (default) The actionable incoming call alert is disabled. The traditional incoming call pop-up alert displays.
- Show for all Incoming Call: The actionable incoming call alert displays for all calls regardless of visibility.
- Show for Invisible Incoming Call: The actionable incoming call alert displays for calls not shown on the phone. This parameter behaves similarly to the incoming call alert pop-up notification.

If you also configure this field in the other windows, the setting precedence is:

1 Device Configuration window settings
2 Common Phone Profile window settings
3 Enterprise Phone Configuration window settings

Step 3 Select **Save**.

Enable the Call History Display Enhancement

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose **Device** > **Phone**.
Step 2 Find your phone from the list of phones associated with the Cisco Unified Communications Manager.
Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.
Step 4 Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose **Enable**.
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings
2 Common Phone Profile window settings
3 Enterprise Phone Configuration window settings

Enable Call History for Shared Line

For more information, see *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 Go to Cisco Unified CM Administration and choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones associated with the Cisco Unified CM.

Step 3 Click on the Device Name of the phone.

Step 4 Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose the applicable profile.
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1. Device Configuration window settings
2. Common Phone Profile window settings
3. Enterprise Phone Configuration window settings

Set Up the Default Line Filter

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose **Device** > **Phone**.

Step 2 Locate the Default Line Filter field and enter the line DN. Separate device name entries with a comma.
The specified line is added to the default filter.

Set Up Custom Line Filter

The Custom Line Filter feature provides configurable options that help reduce alert activity by filtering it to high-priority lines as desired. Only you can configure or edit the default phone filter.

When the default line filter is configured, a filter named Daily schedule is available to users under the Call notifications options in the **Settings** > **Preferences** menu of the phone. This daily schedule filter is in addition to the preset All Calls filter.

If the default line filter is not configured, the phone checks all provisioned lines. If configured, the phone checks the lines set on Cisco Unified Communications Manager if the user selects Default filter as the active filter, or if there are no custom filters.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Set the Default line filter field.
A comma-separated list of phone device names to be included in the default filter.

By default, the list is blank, and all provisioned lines are checked.

Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons. Call-handling features that can be assigned to buttons include Answer, Mobility, and All Calls.

Ideally, you modify templates before you register phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

Modify Phone Button Template

For more information about IP Phone services, see "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see "Cisco Unified IP Phone Configuration" chapter and "Configuring Speed-Dial Buttons" section in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find**.

Step 3 Select the phone model.

Step 4 Select **Copy**, enter a name for the new template, and then select **Save**.
The Phone Button Template Configuration window opens.

Step 5 Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.

Step 6 Select **Save** to create a new phone button template that uses the service URL.

Step 7 Choose **Device** > **Phone** and open the Phone Configuration window for the phone.

Step 8 Select the new phone button template from the Phone Button Template drop-down list.

Step 9 Select **Save** to store the change and then select **Apply Config** to implement the change.
The phone user can now access the Self Care Portal and associate the service with a button on the phone.

Assign Phone Button Template for All Calls

Assign an All Calls button in the phone template for users with multiple shared lines.

When you configure an All Calls button on the phone, users use the All Calls button to:

- See a consolidated list of current calls from all lines on the phone.
- See (under Call History) a list of all missed calls from all lines on the phone.
- Place a call on the user's primary line when the user goes off-hook. All Calls automatically defaults to the user primary line for any outgoing call.

Procedure

Step 1 Modify the phone button template to include the All Calls button.

Step 2 Assign the template to the phone.

Set Up PAB or Speed Dial as IP Phone Service

You can modify a phone button template to associate a service URL with a programmable button. Doing so provides users with single-button access to the PAB and Speed Dials. Before you modify the phone button template, you must configure PAB or Speed Dials as an IP Phone service.

To configure PAB or Speed Dial as an IP Phone service (if it is not already a service), follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.
The Find and List IP Phone Services window displays.

Step 2 Click **Add New**.
The IP Phone Services Configuration window displays.

Step 3 Enter the following settings:

- Service Name: Enter **Personal Address Book**.
- Service Description: Enter an optional description of the service.
- Service URL

  For PAB, enter the following URL:

  http://<Unified CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  For Fast Dial, enter the following URL:

  http://<Unified-CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Secure Service URL

  For PAB, enter the following URL:

  https://<Unified CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  For Fast Dial, enter the following URL:

  https://<Unified-CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Service Category: Select **XML Service**.
- Service Type: Select **Directories**.
- Enable: Select the check box.

  http://<IP_address> or *https://<IP_address>* (Depends on the protocol that the Cisco IP Phone supports.)

Step 4 Select **Save**.
You can add, update, or delete service parameters as described in the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note If you change the service URL, remove an IP Phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes; otherwise, users must resubscribe to the service to rebuild the correct URL.

Modify Phone Button Template for PAB or Fast Dial

You can modify a phone button template to associate a service URL with a programmable button. Doing so provides users with single-button access to the PAB and Speed Dials. Before you modify the phone button template, you must configure PAB or Speed Dials as an IP Phone service.

For more information about IP Phone services, see "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see "Cisco Unified IP Phone Configuration" chapter and "Configuring Speed-Dial Buttons" section in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find**.

Step 3 Select the phone model.

Step 4 Select **Copy**, enter a name for the new template, and then select **Save**.
The Phone Button Template Configuration window opens.

Step 5 Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.

Step 6 Select **Save** to create a new phone button template that uses the service URL.

Step 7 Choose **Device** > **Phone** and open the Phone Configuration window for the phone.

Step 8 Select the new phone button template from the Phone Button Template drop-down list.

Step 9 Select **Save** to store the change and then select **Apply Config** to implement the change.
The phone user can now access the Self Care Portal and associate the service with a button on the phone.

Control Phone Web Page Access

For security purposes, access to the phone web pages is disabled by default. This practice prevents access to the phone web pages and the Cisco Unified Communications Self Care Portal.

Note Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Specify the criteria to find the phone and select **Find**, or select **Find** to display a list of all phones.

Step 3 Select the device name to open the Phone Configuration window for the device.

Step 4 Scroll to the Product Specific Configuration area.

Step 5 To enable access, from the Web Access drop-down list, choose **Enabled**.

Step 6 To disable access, from the Web Access drop-down list, choose **Disabled**.

Step 7 Select **Save**.

Related Topics

Access Web Page for Phone

Set Up Softkey Template

Using Cisco Unified Communications Manager Administration, you can associate a maximum of 18 softkeys with applications that are supported by the phone. Cisco Unified Communications Manager supports the Standard User and Standard Feature softkey template.

An application that supports softkeys has one or more standard softkey templates associated with it. You modify a standard softkey template by copying it, renaming it, and then updating the new template. You can also modify a nonstandard softkey template.

The Softkey Control parameter shows if softkeys of a phone are controlled by the Feature Control Policy or the Softkey Template feature. The Softkey Control parameter is a required field.

The default is Feature Control Policy.

For more information about configuring this feature, see the *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter, and the *Cisco Unified Communications Manager System Guide*, "Softkey Template" chapter.

The Cisco IP Phones do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager allows you to enable or disable some softkeys in the control policy configuration settings. The following table lists the features and the softkeys that can be configured on a softkey template, and identifies whether it is supported on the Cisco IP Phones.

Note Cisco Unified Communications Manager allows you to configure any softkey in a softkey template, but unsupported softkeys do not display on the phone.

Table 27: Configurable Softkeys

Feature	Configurable Softkeys in the Softkey Template configuration	Supported as a Softkey	Notes
Answer	Answer (Answer)	Yes	—
Call Back	Call Back (CallBack)	Yes	—
Call Forward All	Forward All (cfwdAll)	Yes	Phone displays Forward all or Forward off.
Call Park	Call Park (Park)	Yes	—
Call Pickup	Pick Up (Pickup)	Yes	—
cBarge	Conference Barge (Merge)	Yes	cBarge uses the Cisco Unified Communications Manager conference bridge. The softkey label is Merge.
Conference	Conference (Confrn)	Yes	Conference is a dedicated button.

Feature	Configurable Softkeys in the Softkey Template configuration	Supported as a Softkey	Notes
Conference List	Conference List (ConfList)	Yes	Phone displays Show detail.
Divert	Immediate Divert (iDivert)	Yes	Phone displays Decline.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure Do Not Disturb as a programmable line button or as a softkey.
End Call	End Call (EndCall)	Yes	—
Group Pickup	Group Pick UP (GPickUp)	Yes	—
Hold	Hold (Hold)	Yes	Hold is a dedicated button.
Hunt Group	HLog (HLog)	Yes	Configure Hunt Group as a programmable feature button.
Join	Join (Join)	No	—
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure Malicious Call Identification as a programmable feature button or as a softkey.
Meet Me	Meet Me (MeetMe)	Yes	—
Mobile Connect	Mobility (Mobility)	Yes	Configure Mobile Connect as a softkey.
New Call	New Call (NewCall)	Yes	—
Other Pickup	Other Pickup (oPickup)	Yes	—
PLK Support for Queue Statistics	Queue Status	No	—
Quality Reporting Tool	Quality Reporting Tool (QRT)	Yes	Configure Quality Reporting Tool as a programmable feature button or as a softkey.
Redial	Redial (Redial)	Yes	—
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	No	—

Feature	Configurable Softkeys in the Softkey Template configuration	Supported as a Softkey	Notes
Resume	Resume (Resume)	Yes	—
Select	Select (Select)	No	—
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays SpeedDial.
Transfer	Transfer (Trfr)	Yes	Transfer is a dedicated button.
Video Mode Command	Video Mode Command (VidMode)	No	—

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select one of the following windows:

- To configure softkey templates, select **Device** > **Device Settings** > **Softkey Template**.
- To assign a softkey template to a phone, select **Device** > **Phone** and configure the Softkey Template field.

Step 2 Save the changes.

Set Up RTP/sRTP Port Range

You configure the Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP) port values in the SIP profile. RTP and sRTP port values range from 2048 to 65535, with a default range of 16384 to 32764. Some port values within the RTP and sRTP port range are designated for other phone services. You cannot configure these ports for RTP and sRTP.

For more information, see the "SIP profile setup" chapter, in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 Select **Device** > **Device Settings** > **SIP Profile**

Step 2 Choose the search criteria to use and click **Find**.

Step 3 Select the profile to modify.

Step 4 Set the Start Media Port and Stop Media Port to contain the start and end of the port range.

The following list identifies the UDP ports that are used for other phone services and thus not available for RTP and sRTP use:

port 4051

used for the Peer Firmware Sharing (PFS) feature

port 5060

used for SIP over UDP transport

port range 49152 to 53247

used for local ephemeral ports

port range 53248 to 65535

used for the VxC single tunnel VPN feature

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Set Up TLS Resumption Timer

TLS Session resumption enables a TLS session to resume without repeating the entire TLS authentication process. It can significantly reduce the time taken for TLS connection to exchange data.

Although the phones support TLS sessions, all TLS sessions do not support TLS resumption. The following list describes the different sessions and TLS resumption support:

- TLS session for SIP signaling: supports resumption
- HTTPs client: supports resumption
- CAPF: supports resumption
- TVS: supports resumption
- EAP-TLS: does not support resumption
- EAP-FAST: does not support resumption
- VPN client: does not support resumption

For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Set the TLS Resumption Timer parameter.

The range for the timer is 0 to 3600 sec. The default value is 3600. If the field is set to 0, then TLS session resumption is disabled.

Set Up Visual Voicemail

Visual Voicemail is configured for all Cisco IP Phones or to an individual user or group of users, from the Cisco Unified Communications Manager Administration.

Note For configuration information, see the Cisco Visual Voicemail documentation at http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Select **Add New** to create a new service for Visual Voicemail.

Step 3 In the IP Phone Service Configuration window, enter the following information in their respective fields:

- Service Name. Enter Bigeasy_VisualVoicemail.
- ASCII Service Name. Enter Bigeasy_VisualVoicemail.
- Service URL. Enter as Application:Cisco/VisualVoiceMail.
- Service Category. Select XML Service from the pulldown menu.
- Service Type. Select Messages from the pulldown menu.

Step 4 Check **Enable** and click **Save**.

Note Ensure that you do not check **Enterprise Subscription**.

Step 5 In the Service Parameter Information window, click **New Parameter** and enter the following information in their respective fields:

- Parameter Name. Enter voicemail_server.
- Parameter Display Name. Enter voicemail_server.
- Default Value. Enter the hostname of the primary Unity Server.
- Parameter Description

Step 6 Check **Parameter is Required** and click **Save**.

Note Ensure that you do not check **Parameter is a Password (mask contents)**.

Step 7 Close the window and select **Save** again in the Phone Service Configuration window.

Set Up Visual Voicemail for a Specific User

Use the following procedure to configure Visual Voicemail for a specific user.

Note For configuration information, see the Cisco Visual Voice Mail documentation at http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Select the device associated to the user you are searching for.

Step 3 In the Related Links drop-down, choose **Sunscribe/Unsubscribe Services** and click **Go**.

Step 4 Select the VisualVoiceMail Service you created, then choose **Next** > **Subscribe**.

Visual Voicemail Setup for a User Group

To add a batch of Cisco IP Phones 8811, 8841, 8851 and 8861 to Cisco Unified Communications Manager with Visual Voicemail subscribed, create a phone template in BAT tool for each phone type and in each phone template. You can then subscribe to the Visual Voicemail service, and use the template to insert the phones.

If you already have Cisco IP Phones 8811, 8841, 8851 and 8861 phones registered and want to get phones subscribed to the Visual Voicemail service, create a phone template in BAT, subscribe to the Visual Voicemail service in the template, and then use BAT tool to update phones.

For more information, see http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Enable Intelligent Proximity

Intelligent Proximity enables users to take advantage of the acoustic properties of the phone with their mobile device or tablet. The user pairs the mobile device or tablet to the phone using Bluetooth.

With a mobile device paired, the user can place and receive mobile calls on the phone. With a tablet, the user can route the audio from the tablet to the phone.

Users can pair multiple mobile devices, tablets, and a Bluetooth headset to the phone. However, only one device and one headset can be connected at the same time.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Phone** > **Device**.
Step 2 Locate the phone you want to modify.
Step 3 Locate the Bluetooth field and set the field to **Enabled**.
Step 4 Locate the Allow Bluetooth Mobile Handsfree Mode field, and set the field to **Enabled**.
Step 5 Save the changes and apply them to the phone.

Manage Join Across Lines and Transfer Across Lines

The Join Across Lines (JAL) feature allows a user to join calls on multiple phone lines (either on different directory numbers or on the same directory number but on different partitions) to create a conference. The Transfer Across Lines (TAL) feature allows a user to transfer one established call to another established call (either on different phone lines or on the same line). You can disable the JAL and TAL features to avoid users joining or transferring calls by mistake.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select one of the following windows:

- **Device** > **Phone**
- **Device** > **Device Settings** > **Common Phone Profile**
- **System** > **Enterprise Phone**

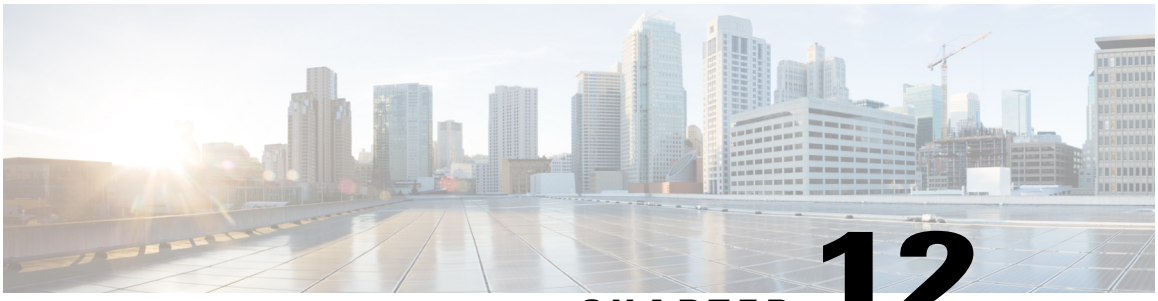
If you configure the parameter in multiple windows, the precedence order is:

1 **Device** > **Phone**
2 **Device** > **Device Settings** > **Common Phone Profile**
3 **System** > **Enterprise Phone**

Step 2 If required, locate the phone.
Step 3 Locate the Join and Direct Transfer Policy field and select one of the following settings:

- Same line, across line enable (default)
- Same line enable
- Same line, across line disable

Step 4 Select **Save**.



CHAPTER 12

Corporate and Personal Directory

- Corporate Directory Setup, page 205
- Personal Directory Setup, page 205
- User Personal Directory Entries Setup, page 206

Corporate Directory Setup

The Corporate Directory allows a user to look up phone numbers for coworkers. To support this feature, you must configure corporate directories.

Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified Communications Manager applications that interface with Cisco Unified Communications Manager. Authentication establishes user rights to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific phone extension.

For more information, see "Understanding Directory Numbers" in the *Cisco Unified Communications Manager System Guide*.

After you complete the LDAP directory configuration, users can use the Corporate Directory service on their phone to look up users in the corporate directory.

Personal Directory Setup

The Personal Directory allows a user to store a set of personal numbers.

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Speed Dials
- Address Book Synchronization Tool (TABSynch)

Users can use these methods to access Personal Directory features:

- From a web browser: Users can access the PAB and Speed Dials features from the Cisco Unified Communications Self Care Portal.

- From the Cisco IP Phone: Choose Contacts to search the corporate directory or the user personal directory.
- From a Microsoft Windows application: Users can use the TABSynch tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the WAB. TabSync can then be used to synchronize the WAB with Personal Directory. For instructions about TABSync, see Download Cisco IP Phone Address Book Synchronizer, on page 206 and Set Up Synchronizer, on page 207.

To ensure that Cisco IP Phone Address Book Synchronizer users access only their end-user data, activate the Cisco UXL Web Service in Cisco Unified Serviceability.

To configure Personal Directory from a web browser, users must access their Self Care Portal. You must provide users with a URL and sign-in information.

User Personal Directory Entries Setup

Users can configure personal directory entries on the Cisco IP Phone. To configure a personal directory, users must have access to the following:

- Self Care Portal: Make sure that users know how to access their Self Care Portal. See Set Up Access to Self Care Portal, on page 80 for details.
- Cisco IP Phone Address Book Synchronizer: Make sure to provide users with the installer. See Download Cisco IP Phone Address Book Synchronizer, on page 206.

Download Cisco IP Phone Address Book Synchronizer

To download a copy of the synchronizer to send to your users, follow these steps:

Procedure

Step 1 To obtain the installer, choose **Application** > **Plugins** from Cisco Unified Communications Manager Administration.

Step 2 Select **Download**, which is located next to the Cisco IP Phone Address Book Synchronizer plugin name.

Step 3 When the file download dialog box displays, select **Save**.

Step 4 Send the TabSyncInstall.exe file and the instructions in Cisco IP Phone Address Book Synchronizer Deployment, on page 206 to all users who require this application.

Cisco IP Phone Address Book Synchronizer Deployment

The Cisco IP Phone Address Book Synchronizer synchronizes data that is stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the Self Care Portal Personal Address Book.

Tip To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before you perform the following procedures.

Install Synchronizer

To install the Cisco IP Phone Address Book Synchronizer, follow these steps:

Procedure

Step 1 Get the Cisco IP Phone Address Book Synchronizer installer file from your system administrator.

Step 2 Double-click the TabSyncInstall.exe file that your administrator provided.
The publisher dialog box displays.

Step 3 Select **Run**.
The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.

Step 4 Select **Next**.
The License Agreement window displays.

Step 5 Read the license agreement information, and select the **I Accept**. Select **Next**.
The Destination Location window displays.

Step 6 Choose the directory in which you want to install the application and select **Next**.
The Ready to Install window displays.

Step 7 Select **Install**.
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8 Select **Finish**.

Step 9 To complete the process, follow the steps in Set Up Synchronizer, on page 207.

Set Up Synchronizer

To configure the Cisco IP Phone Address Book Synchronizer, perform these steps:

Procedure

Step 1 Open the Cisco IP Phone Address Book Synchronizer.
If you accepted the default installation directory, you can open the application by choosing **Start** > **All Programs** > **Cisco Systems** > **TabSync**.

Step 2 To configure user information, select **User**.
The Cisco Unified CallManager User Information window displays.

Step 3 Enter the Cisco IP Phone user name and password and select **OK**.

Step 4 To configure Cisco Unified Communications Manager server information, select **Server**.
The Configure Cisco Unified CallManager Server Information window displays.

Step 5 Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and select **OK**.
If you do not have this information, contact your system administrator.

Step 6 To start the directory synchronization process, select **Synchronize**.
The Synchronization Status window provides the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays.

Step 7 Choose the entry that you want to include in your Personal Address Book and select **OK**.

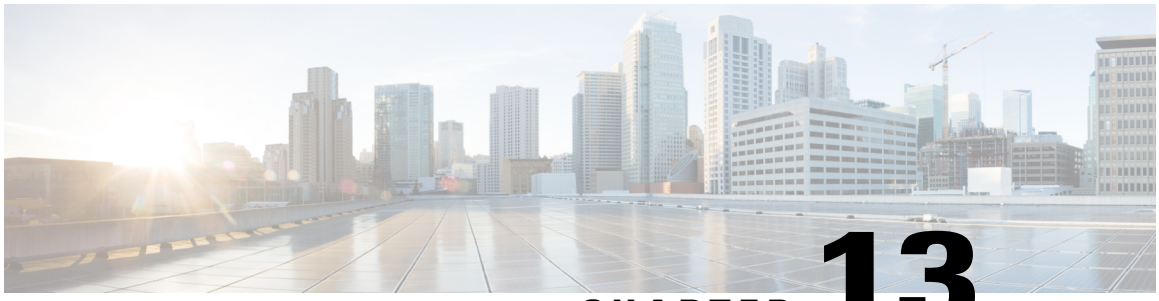
Step 8 When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.

Step 9 To verify whether the synchronization worked, sign in to your Self Care Portal and choose **Personal Address Book**. The users from your Windows address book should be listed.

PART V

Cisco IP Phone Troubleshooting

- Monitoring Phone Systems, page 211
- Troubleshooting, page 245
- Maintenance, page 263
- International User Support, page 269



CHAPTER 13

Monitoring Phone Systems

- Cisco IP Phone Status, page 211
- Cisco IP Phone Web Page, page 229
- Request Information from the Phone in XML, page 242

Cisco IP Phone Status

This section describes how to view model information, status messages, and network statistics on the Cisco IP Phone 8841, 8851, and 8861.

- Model Information: Displays hardware and software information about the phone.
- Status menu: Provides access to screens that display the status messages, network statistics, and statistics for the current call.

You can use the information that displays on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone web page. For more information, see Cisco IP Phone Web Page.

For more information about troubleshooting the Cisco IP Phone 8841, 8851, and 8861, see Troubleshooting, on page 245.

Display Model Information Window

To display the Model Information screen, follow these steps.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Phone Information**.
If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

Step 3 To exit the Model Information screen, press **Exit**.

Related Topics

Cisco IP Phone Web Page

Model Information Fields

The following table describes the Model Information settings.

Table 28: Model Information Settings

Option	Description
Model number	Model number of the phone.
IPv4 Address	IP address of the phone.
Host name	Host name of the phone.
Active load	Version of firmware currently installed on the phone. The user can press **Details** for more information.
Inactive load	Inactive load appears only when a download is in progress. A download icon and a status of "Upgrade in Progress" or "Upgrade Failed" also display. If a user presses **Details** during an upgrade, the download filename and components are listed. A new firmware image can be set to download in advance of a maintenance window. Thus instead of waiting for all of the phones to download the firmware, the system switches more rapidly between resetting an existing load to Inactive status and installing the new load. When the download is complete, the icon changes to indicate the completed status; and a check mark displays for a successful download, or an "X" displays for a failed download. If possible, the rest of the loads continue to download.
Last upgrade	Date of the most recent firmware upgrade.
Active server	Domain name of the server to which the phone is registered.
Stand-by server	Domain name of the standby server.

Display Status Menu

The Status menu includes the following options, which provide information about the phone and phone operations:

- Status Messages: Displays the Status Messages screen, which shows a log of important system messages.

- Ethernet Statistic: Displays the Ethernet Statistics screen, which shows Ethernet traffic statistics.
- Wireless Statistics: Displays the Wireless Statistics screen, if applicable.
- Call Statistics: Displays counters and statistics for the current call.
- Current Access Point: Displays the Current Access Point screen, if applicable.

To display the Status menu, perform these steps:

Procedure

Step 1 To display the Status menu, press **Applications**.
Step 2 Select **Admin Settings** > **Status**.
Step 3 To exit the Status menu, press **Exit**.

Display Status Messages Window

The Status Messages window displays the 30 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up.

Procedure

Step 1 Press **Applications** .
Step 2 Select **Admin Settings** > **Status** > **Status Messages**.
Step 3 To remove the current status messages, press **Clear List**.
Step 4 To exit the Status Messages screen, press **Exit**.

Related Topics

Phone Displays Error Messages, on page 248

Status Messages Fields

The following table describes the status messages that display on the Status Messages screen of the phone.

Table 29: Status Messages on the Cisco Unified IP Phone

Message	Description	Possible explanation and action
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.

Message	Description	Possible explanation and action
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down; otherwise, the files may be corrupted.
CTL and ITL installed	The CTL and ITL files are installed on the phone.	None. This message is informational only. Neither the CTL file nor the ITL file was installed previously. For more information about the trust list, see *Cisco Unified Communications Manager Security Guide*.
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. The CTL file was not installed previously. For more information about the CTL file, see the *Cisco Unified Communications Manager Security Guide*.
CTL update failed	The phone could not update the certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, see the *Cisco Unified Communications Manager Security Guide*.
DHCP timeout	DHCP server did not respond.	Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the DHCP server and the phone: Verify the network connections. DHCP server is down: Check configuration of DHCP server. Errors persist: Consider assigning a static IP address.

Message	Description	Possible explanation and action
DNS timeout	DNS server did not respond.	Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the DNS server and the phone: Verify the network connections. DNS server is down: Check configuration of the DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. Consider using IP addresses rather than host names
Duplicate IP	Another device is using the IP address that is assigned to the phone.	If the phone has a static IP address, verify that you did not assigned a duplicate IP address. If you are using DHCP, check the DHCP server configuration.
Erasing CTL and ITL files	Erasing CTL or ITL file.	None. This message is informational only. For more information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management: • Located in subdirectory with same name as network locale: ◦ tones.xml • Located in subdirectory with same name as user locale: ◦ glyphs.xml ◦ dictionary.xml ◦ kate.xml

Message	Description	Possible explanation and action
File not found <Cfg File>	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone does not exist in the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response. • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See Phone Addition Methods, on page 71 for details. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server.
File Not Found <CTLFile.tlv>	This message displays on the phone when the Cisco Unified Communications Manager cluster is not in secure mode.	No impact; the phone can still register to Cisco Unified Communications Manager.
IP address released	The phone is configured to release the IP address.	The phone remains idle until it is power cycled or until you reset the DHCP address.
ITL installed	The ITL file is installed in the phone.	None. This message is informational only. The ITL file was not installed previously. For more information about the ITL file, see *Cisco Unified Communications Manager Security Guide*.

Message	Description	Possible explanation and action
Load rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you attempted to install a version of software on this phone that did not support hardware changes on this phone. Check the load ID that is assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Reenter the load that displays on the phone.
No default router	DHCP or static configuration did not specify a default router.	If the phone has a static IP address, verify that the default router is configured. If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	If the phone has a static IP address, verify that the DNS server is configured. If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
No Trust List installed	The CTL file or the ITL file is not installed on the phone.	The trust list is not configured on the Cisco Unified Communications Manager, which does not support security by default. For more information about the trust list, see the *Cisco Unified Communications Manager Security Guide*.
Restart requested by Cisco Unified Communications Manager	The phone is restarting due to on a request from Cisco Unified Communications Manager.	Configuration changes were likely made to the phone in Cisco Unified Communications Manager, and Apply was pressed so that the changes take effect.
TFTP access error	TFTP server is pointing to a directory that does not exist.	If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. If you are using static IP addresses, check configuration of TFTP server.

Message	Description	Possible explanation and action
TFTP error	The phone does not recognize an error code that the TFTP server provided.	Contact Cisco TAC.
TFTP timeout	TFTP server did not respond.	Network is bus: The errors should resolve themselves when the network load reduces. No network connectivity between the TFTP server and the phone: Verify the network connections. TFTP server is down: Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.

Message	Description	Possible explanation and action
Trust List update failed	Update of the CTL and ITL files failed.	Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files. Possible reasons for failure: • Network failure occurred. • TFTP server was down. • The new security token that was used to sign CTL file and the TFTP certificate that was used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone. • Internal phone failure occurred. Possible solutions: • Check network connectivity. • Check whether the TFTP server is active and functioning normally. • If the Transactional Vsam Services (TVS) server is supported on Cisco Unified Communications Manager, check whether the TVS server is active and functioning normally. • Verify whether the security token and the TFTP server are valid. Manually delete the CTL and ITL files if all the preceding solutions fail; reset the phone.
Trust List updated	The CTL file, the ITL file, or both files are updated.	None. This message is informational only. For more information about the trust list, see the *Cisco Unified Communications Manager Security Guide*.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.

Message	Description	Possible explanation and action
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This message indicates the name of the configuration file for the phone.

Display Network Statistics Screen

The Networks Statistics screen displays information about the phone and network performance.

To display the Network Statistics screen, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin Settings**.

Step 3 Select **Status** > **Network Statistics**.

Step 4 To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear List**.

Step 5 To exit the Ethernet Statistics screen, press **Exit**.

Ethernet Statistics Information

The following tables describe the information in the Ethernet Statistics screen.

Table 30: Ethernet Statistics Information

Item	Description
Rx Frames	Number of packets that the phone received.
Tx Frames	Number of packets that the phone sent.
Rx Broadcasts	Number of broadcast packets that the phone received.

Item	Description
Restart Cause	Cause of the last reset of the phone. Specifies one of the following values: • Initialized • TCP-timeout • CM-closed-TCP • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Phone-Re-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • Load Rejected HC • CM-ICMP-Unreach • Phone-Abort
Elapsed Time	Amount of time that has elapsed since the phone last rebooted.
Port 1	Link state and connection of the Network port. For example, Auto 100 Mb Full-Duplex means that the Network port is in a link-up state and has autonegotiated a full-duplex, 100-Mbps connection.
Port 2	Link state and connection of the PC port.
DHCP state (IPv4 / IPv6)	• In IPv4-mode, displays only the DHCPv4 state, such as DHCP BOUND. • In IPv6-mode, displays only the DHCPv6 state, such as ROUTER ADVERTISE., (GOOD IP). • In dual-stack mode, both DHCPv4 and DHCPv6 state information is displayed.

The following tables describe the messages that appear for DHCPv4 and DHCPv6 states.

Table 31: DHCPv4 ethernet statistics messages

DHCPv4 state	Description
CDP INIT	CDP is not bound or WLAN is not in service
DHCP BOUND	DHCPv4 is BOUND
DHCP DISABLED	DHCPv4 is disabled
DHCP INIT	DHCPv4 is INIT
DHCP INVALID	DHCPv4 is INVALID; this is initial state
DHCP RENEWING	DHCPv4 is RENEWING
DHCP REBINDING	DHCPv4 is REBINDING
DHCP REBOOT	DHCPv4 is init-reboot
DHCP REQUESTING	DHCPv4 is requesting
DHCP RESYNC	DHCPv4 is RESYNCH
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 is booting
DHCP UNRECOGNIZED	Unrecognized DHCPv4 state
DISABLED DUPLICATE IP	Duplicated IPv4 Address
DHCP TIMEOUT	DHCPv4 Timeout
IPV4 STACK TURNED OFF	Phone is in IPv6-only mode with IPv4 Stack turned off
ILLEGAL IPV4 STATE	Illegal IPv4 state and should not happen

Table 32: DHCPv6 ethernet statistics messages

DHCPv6 State	Description
CDP INIT	CDP is initializing
DHCP6 BOUND	DHCPv6 is BOUND
DHCP6 DISABLED	DHCPv6 is DISABLED
DHCP6 RENEW	DHCPv6 is renewing

DHCPv6 State	Description
DHCP6 REBIND	DHCPv6 is rebinding
DHCP6 INIT	DHCPv6 is initializing
DHCP6 SOLICIT	DHCPv6 is soliciting
DHCP6 REQUEST	DHCPv6 is requesting
DHCP6 RELEASING	DHCPv6 is releasing
DHCP6 RELEASED	DHCPv6 is released
DHCP6 DISABLING	DHCPv6 is disabling
DHCP6 DECLINING	DHCPv6 is declining
DHCP6 DECLINED	DHCPv6 is declined
DHCP6 INFOREQ	DHCPv6 is INFOREQ
DHCP6 INFOREQ DONE	DHCPv6 is INFOREQ DONE
DHCP6 INVALID	DHCPv6 is INVALID; this is initial state
DISABLED DUPLICATE IPV6	DHCP6 is DISABLED, but DUPLICATE IPV6 DETECTED
DHCP6 DECLINED DUPLICATE IP	DHCP6 is DECLINED -- DUPLICATE IPV6 DETECTED
ROUTER ADVERTISE., (DUPLICATE IP)	Duplicated autoconfigured IPv6 address
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 is booting
DHCP6 TIMEOUT USING RESTORED VAL	DHCPv6 timeout, using the value saved in flash memory
DHCP6 TIMEOUT CANNOT RESTORE	DHCP6 timeout and there is no backup from flash memory
IPV6 STACK TURNED OFF	Phone is in IPv4-only mode with IPv6 Stack turned off
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6 Address is not from router or DHCPv6 server

DHCPv6 State	Description
ILLEGAL IPV6 STATE	Illegal IPv6 state and should not happen

Display Wireless Statistics Screen

This procedure only applies to the wireless Cisco IP Phone 8861.

To display the Wireless Statistics screen, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin Settings**.

Step 3 Select **Status** > **Wireless Statistics**.

Step 4 To reset the Wireless statistics to 0, press **Clear List**.

Step 5 To exit the Wireless Statistics screen, press **Exit**.

WLAN Statistics

The following table describes the WLAN statistics on the phone.

Table 33: WLAN Statistics on the Cisco Unified IP Phone

Item	Description
Transmit Frames	Number of packets that the phone transmitted.
Directed Frames Received	Number of directed packets that the phone received.
Multicast Frames Received	Number of multicast packets that the phone received.
Broadcast Frames Received	Number of broadcast packets that the phone received.
Receive Errors	Number of packets with errors that the phone received.
Receive No Buffers	The phone has no buffers available to receive the packet.
Frame Checksum (FCS) Errors	Increments when an FCS error is detected in a received MPDU.
Duplicate Frames	Number of duplicate packets received by the phone.
Fragments Received	Number of fragmented packets that the phone received.
Beacons Received	Number of beacons that the phone received.
Association Rejected	Number of AP association rejections that the phone received.

Item	Description
Association Timeouts	Number of AP association timeouts that the phone received.
Authentication Rejects	Number of authentication rejects that the phone received.
Authentication Timeouts	Number of authentication timeouts that the phone received.
QOS Null Frames	Number of QOS null packets that the phone received.
The following WLAN Statistics items display these AP queues: Background (BK), Best Effort (BE), Video (VI), and Voice (VO)	
QOS Data Received	Number of QOS packets that the phone received.
Transmit Ok	Number of packets that the phone transmitted without error.
Transmit Errors	Number of packets with errors that the phone transmitted.
Direct Frames Transmitted	Number of direct packets that the phone transmitted.
Multicast Frames Transmitted	Number of multicast packets that the phone transmitted.
Broadcast Frames Transmitted	Number of broadcast packets that the phone transmitted.
RTS Failed	A corresponding CTS was not received.
ACK Failed	AP did not acknowledge a transmission.
Retries	Counter of total retries.
Multiple Retries	Transmission of packet required two or more retries before success.
Retry Failures	Transmission of packet failed.
Transmit Timeouts	Transmission of packet failed due to queue time.
Success Counter	Counter of successful transmissions.
Max Retry Failure	Counter of successive transmission failures that caused a roaming attempt.

Display Call Statistics Window

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics of the most recent call.

Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone. For more information about remote monitoring, see Cisco IP Phone Web Page.

A single call can use multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings** > **Status** > **Call Statistics**.

Step 3 To exit the Call Statistics screen, press **Exit**.

Call Statistics Fields

The following table describes the items on the Call Statistics screen.

Table 34: Call Statistics items for the Cisco Unified Phone

Item	Description
Receiver codec	Type of received voice stream (RTP streaming audio from codec): G.729, G.722, G.711 mu-law, G.711 A-law, and iLBC.
Sender codec	Type of transmitted voice stream (RTP streaming audio from codec): G.729, G.722, G.711 mu-law, G.711 A-law, and iLBC.
Receiver size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Receiver packets	Number of RTP voice packets that were received since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were received since the call began because the call might have been placed on hold.
Sender packets	Number of RTP voice packets that were transmitted since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were transmitted since the call began because the call might have been placed on hold.

Item	Description
Avg jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving voice stream opened.
Max jitter	Maximum jitter, in milliseconds, that was observed since the receiving voice stream opened.
Receiver discarded	Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on). **Note** The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.
Receiver lost packets	Missing RTP packets (lost in transit).
Voice-Quality Metrics	
Cumulative conceal ratio	Total number of concealment frames divided by total number of speech frames that were received from start of the voice stream.
Interval conceal ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max conceal ratio	Highest interval concealment ratio from start of the voice stream.
Conceal seconds	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely conceal seconds	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

Display Current Access Point Window

The Current Access Point screen displays statistics about the access point that the Cisco IP Phone 8861 uses for wireless communications. Current Access Point Fields describes the information that appears in this screen.

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin Settings** > **Status** > **Current Access Point**.

Step 3 To exit the Current Access Point screen, press **Exit**.

Current Access Points Fields

The following table describes the fields in the Current Access Point screen.

Table 35: Current Access Point Items

Item	Description
AP name	Name of the AP, if it is CCX-compliant; otherwise, the MAC address displays here.
MAC address	MAC address of the AP.
Frequency	The latest frequency where this AP was observed.
Current channel	The latest channel where this AP was observed.
Last RSSI	The latest RSSI in which this AP was observed.
Beacon interval	Number of time units between beacons. A time unit is 1.024 ms.
Capability	This field contains a number of subfields that are used to indicate requested or advertised optional capabilities.
Basic rates	Data rates that the AP requires and the AP at which the station must be capable of operating.
Optional rates	Data rates that the AP supports and the AP that are optional for the station to operate at.
DTIM period	Every nth beacon is a dtime period. After each DTIM beacon, the AP sends any broadcast or multicast packets that are queued for power-save devices.
Country code	A two-digit country code. Country information might not be display if the country information element (IE) is not present in the beacon.
Channels	A list of supported channels (from the country IE).
Power constraint	The amount of power by which the maximum transmit power should be reduced from the regulatory domain limit.
Power limit	Maximum transmit power in dBm that is permitted for that channel.

Item	Description
Channel utilization	The percentage of time, normalized to 255, in which the AP sensed the medium was busy, as indicated by the physical or virtual carrier sense (CS) mechanism.
Station count	Data rates that the AP requires and at which the station must be capable of operating.
Admission capacity	An unsigned integer that specifies the remaining amount of medium time that is available through explicit admission control, in units of 32 microseconds per second. If the value is 0, the AP does not support this information element and the capacity is unknown.
WMM supported	Support for Wi-Fi multimedia extensions.
UAPSD Supported	The AP supports Unscheduled Automatic Power Save Delivery. May only be available if WMM is supported. This feature is critical for talk time and for achieving maximum call density on the wireless IP Phone.
Proxy ARP	CCX-compliant AP supports responding to IP ARP requests on behalf of the associated station. This feature is critical to standby time on the wireless IP Phone.
CCX version	If the AP is CCX compliant, this field shows the CCX version.
Best Effort	Contains information related to the Best Effort queue.
Background	Contains information related to the Background queue.
Video	Contains information related to the Video queue.
Voice	Contains information related to the Voice queue.

Cisco IP Phone Web Page

Each Cisco IP Phone has a web page from which you can view a variety of information about the phone, including:

- Device information: Displays device settings and related information for the phone.
- Network setup: Displays network setup information and information about other phone settings.
- Network statistics: Displays hyperlinks that provide information about network traffic.
- Device logs: Displays hyperlinks that provide information that you can use for troubleshooting.
- Streaming statistic: Displays hyperlinks that display a variety of streaming statistics.
- System: Displays a hyperlink to restart the phone.

This section describes the information that you can obtain from the phone web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information directly from a phone.

Access Web Page for Phone

To access the web page for a Cisco IP Phone, follow these steps:

Note If you cannot access the web page, it may be disabled by default.

Procedure

Step 1 Obtain the IP address of the Cisco IP Phone by using one of these methods:

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device** > **Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.

b) On the Cisco IP Phone, press **Applications**, choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**, and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco IP Phone: **http://**<IP_address>

Device Information

The Device information area on a phone web page displays device settings and related information for the phone. The following table describes these items.

Note Some of the items in the following table do not apply to all phone models.

To display the Device information area, access the web page for the phone as described in Access Web Page for Phone, on page 230, and then click the Device information hyperlink.

Table 36: Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone.
Host name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Phone DN	Directory number that is assigned to the phone.
Version	Identifier of the firmware that is running on the phone.
Key Expansion Module 1	Identifier for the first KEM, if applicable.

Item	Description
Key Expansion Module 2	Identifier for the second KEM, if applicable.
Key Expansion Module 3	Identifier for the third KEM, if applicable.
Hardware Revision	Revision value of the phone hardware.
Serial Number	Unique serial number of the phone.
Model Number	Model number of the phone.
Message Waiting	Indicates whether is a voice message is waiting on the primary line for this phone.
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device type: Indicates hardware type. For example, phone displays for all phone models. • Device description: Displays the name of the phone associated with the indicated model type. • Product identifier: Specifies the phone model. • Serial number: Displays the unique serial number of the phone.
Key Expansion Module UDI	Cisco Unique Device Identifier (UDI) of the KEM.
Time	Time for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Time Zone	Time zone for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Date	Date for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
FIPS Mode Enabled	Indicates if the Federal Information Processing Standard (FIPS) Mode is enabled.

Network Setup

The Network setup area on a phone web page displays network setup information and information about other phone settings. The following table describes these items.

You can view and set many of these items from the Network Setup menu on the Cisco IP Phone.

To display the Network Setup area, access the web page for the phone as described in Access Web Page for Phone, on page 230, and then click the Network setup hyperlink.

Table 37: Network Setup Area Items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains the IP address.
BOOTP Server	Indicates whether the phone obtains the configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask that the phone uses.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used that the phone uses.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used that the phone uses.
Default Router 1	Default router used that the phone uses.
DNS Server 1–3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2 and 3) that the phone uses.
Operational VLAN ID	Operational Virtual Local Area Network (VLAN) that is configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member.

Item	Description
CUCM Server 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item shows the Cisco Unified Communications Manager server IP address and one of the following states: • Active: Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services • Standby: Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable • Blank: No current connection to this Cisco Unified Communications Manager server An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window.
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
DHCP	Indicates whether the phone uses DHCP.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone is idle for the time that the Idle URL Time field specifies and no menu is open.
Idle URL Time	Number of seconds that the phone is idle and no menu is open before the XML service that the Idle URL specifies activates.
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of the phone HTTP client and provides responses from the nonlocal host to the phone HTTP client.

Item	Description
Authentication URL	URL that the phone uses to validate requests that are made to the phone web server.
SW Port Setup	Speed and duplex of the switch port, where: • A = Auto Negotiate • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • No Link= No connection to the switch port
PC Port Setup	Speed and duplex of the switch port, where: • A = Auto Negotiate • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • No Link = No connection to the PC port
User Locale	User locale that associates with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale that associates with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences that the phone uses.
User Locale Version	Version of the user locale that is loaded on the phone.
Network Locale Version	Version of the network locale that is loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

Item	Description
Video Capability Enabled	Indicates whether the phone can participate in video calls when it connects to an appropriately equipped camera.
Voice VLAN Enabled	Indicates whether the phone allows a device that is attached to the PC port to access the Voice VLAN.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates whether the phone forwards packets that are transmitted and received on the network port to the access port.
PC VLAN	VLAN that identifies and removes 802.1P/Q tags from packets that are sent to the PC.
CDP on PC Port	Indicates whether CDP is supported on the PC port (default is enabled). When CDP is disabled in Cisco Unified Communications Manager, a warning is displays to indicate that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown in the Settings menu.
CDP on SW Port	Indicates whether CDP support exists on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the phone connects to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone connects to a non-Cisco switch. The current PC and switch port CDP values are shown on the Settings menu.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.

Item	Description
LLDP Power Priority	Advertises the phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones. Settings include: • Unknown: This is the default value. • Low • High • Critical
LLDP Asset ID	Identifies the asset ID that is assigned to the phone for inventory management.

Network Statistics

The following Network statistics hyperlinks on a phone web page provide information about network traffic on the phone:

- Ethernet information: Displays information about Ethernet traffic.
- Access: Displays information about network traffic to and from the PC port on the phone.
- Network: Displays information about network traffic to and from the network port on the phone.

To display a Network statistics area, access the web page for the phone, and then click the **Ethernet Information**, the **Access**, or the **Network** hyperlink.

Ethernet Information Web Page

The following table describes the contents of the Ethernet information web page.

Table 38: Ethernet Information Items

Item	Description
Tx Frames	Total number of packets that the phone transmits.
Tx broadcast	Total number of broadcast packets that the phone transmits.
Tx multicast	Total number of multicast packets that the phone transmits.
Tx unicast	Total number of unicast packets that the phone transmits.
Rx Frames	Total number of packets received by the phone.
Rx broadcast	Total number of broadcast packets that the phone receives..
Rx multicast	Total number of multicast packets that the phone receives.
Rx unicast	Total number of unicast packets that the phone receives.

Item	Description
Rx PacketNoDes	Total number of shed packets that the no Direct Memory Access (DMA) descriptor causes.

Access and Network Web Pages

The following table describes the information in the Access and Network web pages.

Table 39: Access and Network Fields

Item	Description
Rx totalPkt	Total number of packets that the phone received.
Rx crcErr	Total number of packets that were received with CRC failed.
Rx alignErr	Total number of packets between 64 and 1522 bytes in length that were received and that have a bad Frame Check Sequence (FCS).
Rx multicast	Total number of multicast packets that the phone received.
Rx broadcast	Total number of broadcast packets that the phone received.
Rx unicast	Total number of unicast packets that the phone received.
Rx shortErr	Total number of received FCS error packets or Align error packets that are less than 64 bytes in size.
Rx shortGood	Total number of received good packets that are less than 64 bytes size.
Rx longGood	Total number of received good packets that are greater than 1522 bytes in size.
Rx longErr	Total number of received FCS error packets or Align error packets that are greater than 1522 bytes in size.
Rx size64	Total number of received packets, including bad packets, that are between 0 and 64 bytes in size.
Rx size65to127	Total number of received packets, including bad packets, that are between 65 and 127 bytes in size.
Rx size128to255	Total number of received packets, including bad packets, that are between 128 and 255 bytes in size.
Rx size256to511	Total number of received packets, including bad packets, that are between 256 and 511 bytes in size.

Item	Description
Rx size512to1023	Total number of received packets, including bad packets, that are between 512 and 1023 bytes in size.
Rx size1024to1518	Total number of received packets, including bad packets, that are between 1024 and 1518 bytes in size.
Rx tokenDrop	Total number of packets that were dropped due to lack of resources (for example, FIFO overflow).
Tx excessDefer	Total number of packets that were delayed from transmitting due to busy medium.
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission.
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
Tx Collisions	Total number of collisions that occurred while a packet was transmitted.
Tx excessLength	Total number of packets that were not transmitted because the packet experienced 16 transmission attempts.
Tx broadcast	Total number of broadcast packets that the phone transmitted.
Tx multicast	Total number of multicast packets that the phone transmitted.
LLDP FramesOutTotal	Total number of LLDP frames that the phone sent out.
LLDP AgeoutsTotal	Total number of LLDP frames that timed out in the cache.
LLDP FramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
LLDP FramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
LLDP FramesInTotal	Total number of LLDP frames that the phone receives.
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded.
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone.
CDP Neighbor Device ID	Identifier of a device connected to this port that CDP discovered.
CDP Neighbor IPv6 address	IP address of the neighbor device discovered that CDP protocol discovered.

Item	Description
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP discovered.
LLDP Neighbor IPv6 address	IP address of the neighbor device that LLDP protocol discovered.
LLDP Neighbor Port	Neighbor device port to which the phone connects that LLDP protocol discovered.
Port Information	Speed and duplex information.

Device Logs

The following Device log hyperlinks on a phone web page provide information that helps to monitor and troubleshoot the phone.

- Console logs: Includes hyperlinks to individual log files. The console log files include debug and error messages that the phone received.
- Core dumps: Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- Status messages: Displays the 10 most recent status messages that the phone has generated since it last powered up. The Status Messages screen on the phone also displays this information.
- Debug display: Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

A Cisco Unified IP Phone can stream information to and from up to three devices simultaneously. A phone streams information when it is on a call or is running a service that sends or receives audio or data.

The Streaming statistics areas on a phone web page provide information about the streams.

The following table describes the items in the Streaming Statistics areas.

Table 40: Streaming Statistics area items

Item	Description
Remote address	IP address and UDP port of the destination of the stream.
Local address	IP address and UPD port of the phone.
Start time	Internal time stamp indicates when Cisco Unified Communications Manager requested that the phone start transmitting packets.

Item	Description
Stream status	Indication of whether streaming is active or not.
Host name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Sender packets	Total number of RTP data packets that the phone transmitted since it started this connection. The value is 0 if the connection is set to receive-only mode.
Sender octets	Total number of payload octets that the phone transmitted in RTP data packets since it started this connection. The value is 0 if the connection is set to receive-only mode.
Sender codec	Type of audio encoding that is for the transmitted stream.
Sender reports sent (see note)	Number of times the RTCP Sender Report has been sent.
Sender report time sent (see note)	Internal time-stamp indication as to when the last RTCP Sender Report was sent.
Rcvr lost packets	Total number of RTP data packets that have been lost since data reception started on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or are duplicates. The value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet interarrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Receiver Codec	Type of audio encoding that is used for the received stream.
Receiver Reports Sent (see note)	Number of times the RTCP Receiver Reports have been sent.
Receiver Report Time Sent (see note)	Internal time-stamp indication as to when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets that the phone has received since data reception started on this connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets that the device received in RTP data packets since reception started on the connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.

Item	Description
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If voice activity detection (VAD) is in use, a longer interval might be required to accumulate three seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from the start of the voice stream.
	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events that are to frame loss in the preceding eight-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 266. **Note** The MOS LQK score can vary due to the codec type that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score that was observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score that was observed from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score that was observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 yields 4.5. • G.729 A /AB yields 3.7.
MOS LQK Version	Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.

Item	Description
Sender Reports Received (see note)	Number of times RTCP Sender Reports have been received.
Sender Report Time Received (see note)	Most recent time when an RTCP Sender Report was received.
Receiver Size	RTP packet size, in milliseconds, for the received stream.
Receiver Discarded	RTP packets that were received from the network but were discarded from the jitter buffers.
Receiver Reports Received (see note)	Number of times RTCP Receiver Reports have been received.
Receiver Report Time Received (see note)	Most recent time when an RTCP Receiver Report was received.

Note When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Request Information from the Phone in XML

For troubleshooting purposes, you can request information from the phone. The resulting information is in XML format. The following information is available:

- CallInfo is call session information for a specific line.
- LineInfo is line configuration information for the phone.
- ModeInfo is phone mode information.

Before You Begin

Web access needs to be enabled to get the information.

The phone must be associated with a user.

Procedure

Step 1 For Call Info, enter the following URL in a browser: http://<phone ip address>/CGI/Java/CallInfo<x> where

- <*phone ip address*> is the IP address of the phone
- <*x*> is the line number to obtain information about.

The command returns an XML document.

Step 2 For Line Info, enter the following URL in a browser: http://<phone ip address>/CGI/Java/LineInfo where

- <*phone ip address*> is the IP address of the phone

The command returns an XML document.

Step 3 For Model Info, enter the following URL in a browser: http://<phone ip address>/CGI/Java/ModeInfo where

- <*phone ip address*> is the IP address of the phone

The command returns an XML document.

Sample CallInfo Output

The following XML code is an example of the output from the CallInfo command.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
     <CallReference>30303060</CallReference>
     <CallDuration>12835</CallDuration>
     <CallStatus>null</CallStatus>
     <CallSecurity>UNAUTHENTICATED</CallSecurity>
     <CallPrecedence>ROUTINE</CallPrecedence>
     <FeatureList/>
   </CiscoIPPhoneCallInfo>
   <VisibleFeatureList>
     <Feature Position="1" Enabled="true" Label="End Call"/>
     <Feature Position="2" Enabled="true" Label="Show Detail"/>
   </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Sample LineInfo Output

The following XML code is an example of the output from the LineInfo command.

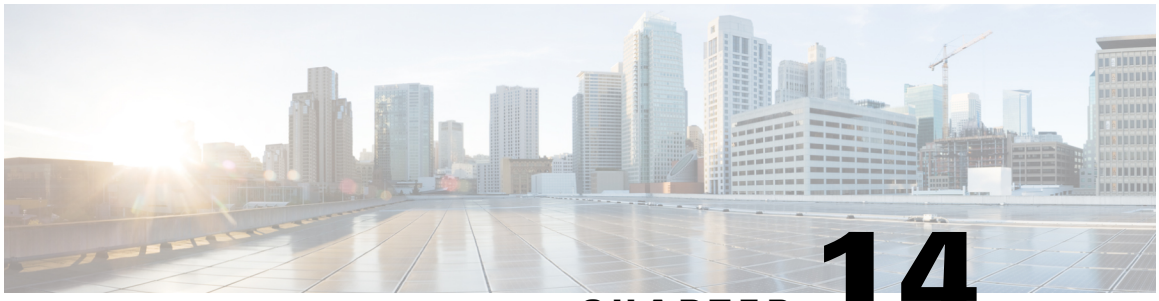
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
```

```
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1029</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1030</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>CONNECTED</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>2</LineType>
     <lineDirNum>9700</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <LineLabel>SD9700</LineLabel>
     <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

Sample ModeInfo Output

The following XML code is an example of the output from the ModeInfo command.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



CHAPTER 14

Troubleshooting

- General Troubleshooting Information, page 245
- Startup Problems, page 247
- Cisco IP Phone Reset Problems, page 250
- Phone Cannot Connect to LAN, page 253
- Cisco IP Phone Security Problems, page 253
- General Telephone Call Problems, page 257
- Troubleshooting Procedures, page 258
- Additional Troubleshooting Information, page 262

General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco IP Phone.

Table 41: Cisco IP Phone troubleshooting

Summary	Explanation
Connecting a Cisco IP Phone to another Cisco IP Phone	Cisco does not support connecting an IP phone to another IP Phone through the PC port. Each IP Phone should connect directly to a switch port. If phones are connected together in a line by using the PC port, the phones do not work.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.

Summary	Explanation
Moving a network connection from the phone to a workstation	If you power your phone through the network connection, you must be careful if you decide to unplug the network connection of the phone and plug the cable into a desktop computer. **Caution** The network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See Apply Phone Password, on page 45 for details. **Note** If the administrator password is not set in common phone profile, then user can modify the network settings.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco IP Phone and the other device. The values of these statistics should match.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to 10 Half (10-BaseT/half duplex). • The phone receives power from an external power supply. • The phone is powered down (the power supply is disconnected). In this case, the switch port on the phone can become disabled and the following message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, reenable the port from the switch.

Startup Problems

After you install a Cisco IP Phone into your network and add it to Cisco Unified Communications Manager, the phone should start up as described in the related topic below.

If the phone does not start up properly, see the following sections for troubleshooting information.

Related Topics

Phone Startup Verification, on page 65

Cisco IP Phone Does Not Go Through Normal Startup Process

Problem

When you connect a Cisco IP Phone to the network port, the phone does not go through the normal startup process as described in the related topic and the phone screen does not display information.

Cause

If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, or the phone may not be functional.

Solution

To determine whether the phone is functional, use the following suggestions to eliminate other potential problems.

- Verify that the network port is functional:
  - Exchange the Ethernet cables with cables that you know are functional.
  - Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.
  - Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.
  - Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.
- Verify that the phone is receiving power:
  - If you are using external power, verify that the electrical outlet is functional.
  - If you are using in-line power, use the external power supply instead.
  - If you are using the external power supply, switch with a unit that you know to be functional.
- If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
- If the phone still does not start up properly, perform a factory reset of the phone.

- After you attempt these solutions, if the phone screen on the Cisco IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Related Topics

Phone Startup Verification, on page 65

Cisco IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages that displays on the phone screen, the phone is not starting up properly. The phone cannot successfully start up unless it connects to the Ethernet network and it registers with a Cisco Unified Communications Manager server.

In addition, problems with security may prevent the phone from starting up properly. See Troubleshooting Procedures, on page 258 for more information.

Phone Displays Error Messages

Problem

Status messages display errors during startup.

Solution

While the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem.

Related Topics

Display Status Messages Window, on page 213

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager

Problem

If the network is down between the phone and either the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly.

Solution

Ensure that the network is currently running.

Phone Cannot Connect to TFTP Server

Problem

The TFTP server settings may not be correct.

Solution

Check the TFTP settings.

Related Topics

Check TFTP Settings, on page 258

Phone Cannot Connect to Server

Problem

The IP addressing and routing fields may not be configured correctly.

Solution

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

Related Topics

Check DHCP Settings, on page 259

Phone Cannot Connect Using DNS

Problem

The DNS settings may be incorrect.

Solution

If you use DNS to access the TFTP server or Cisco Unified Communications Manager, you must ensure that you specify a DNS server.

Cisco Unified Communications Manager and TFTP Services Are Not Running

Problem

If the Cisco Unified Communications Manager or TFTP services are not running, phones may not be able to start up properly. In such a situation, it is likely that you are experiencing a systemwide failure, and other phones and devices are unable to start up properly.

Solution

If the Cisco Unified Communications Manager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see Start Service, on page 261.

Configuration File Corruption

Problem

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

Solution

Create a new phone configuration file. See Create New Phone Configuration File, on page 260 for details.

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with the Cisco Unified Communications Manager

Solution

A Cisco IP Phone can register with a Cisco Unified Communications Manager server only if the phone is added to the server or if autoregistration is enabled. Review the information and procedures in Phone Addition Methods, on page 71 to ensure that the phone is added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device** > **Phone** from Cisco Unified Communications Manager Administration. Click **Find** to search for the phone based on the MAC Address. For information about determining a MAC address, see Determine Phone MAC Address, on page 70.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 250 for assistance.

Cisco IP Phone Cannot Obtain IP Address

Problem

If a phone cannot obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone connects may be disabled.

Solution

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure that the switch port is enabled.

Cisco IP Phone Reset Problems

If users report that their phones are resetting during calls or while the phones are idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco IP Phone should not reset.

Typically, a phone resets if it has problems in connecting to the Ethernet network or to Cisco Unified Communications Manager.

Phone Resets Due to Intermittent Network Outages

Problem

Your network may be experiencing intermittent outages.

Solution

Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

Phone Resets Due to DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

Verify that you have properly configured the phone to use DHCP. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. Cisco recommends that you set the lease duration to 8 days.

Related Topics

Check DHCP Settings, on page 259

Phone Resets Due to Incorrect Static IP Address

Problem

The static IP address assigned to the phone may be incorrect.

Solution

If the phone is assigned a static IP address, verify that you have entered the correct settings.

Phone Resets During Heavy Network Usage

Problem

If the Cisco IP Phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.

Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

Phone Resets Intentional Reset

Problem

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

Solution

You can check if a Cisco IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **Applications** on the phone and choosing **Administrator Settings** > **Status** > **Network Statistics**.

- If the Restart Cause field displays `Reset-Reset`, the phone receives a Reset/Reset from Cisco Unified Communications Manager Administration.
- If the Restart Cause field displays `Reset-Restart`, the phone closed because it received a Reset/Restart from Cisco Unified Communications Manager Administration.

Phone Resets Due to DNS or Other Connectivity Issues

Problem

The phone reset continues and you suspect DNS or other connectivity issues.

Solution

If the phone continues to reset, eliminate DNS or other connectivity errors by following the procedure in Determine DNS or Connectivity Issues, on page 259.

Phone Does Not Power Up

Problem

The phone does not appear to be powered up.

Solution

In most cases, a phone restarts if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then connects to an external power supply.

Phone Cannot Connect to LAN

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

Cisco IP Phone Security Problems

The following sections provide troubleshooting information for the security features on the Cisco IP Phone. For information about the solutions for any of these issues, and for additional troubleshooting information about security, see *Cisco Unified Communications Manager Security Guide*.

CTL File Problems

The following sections describe troubleshooting problems with the CTL file.

Authentication Error, Phone Cannot Authenticate CTL File

Problem

A device authentication error occurs.

Cause

CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.

Solution

Install a correct certificate.

Phone Cannot Authenticate CTL File

Problem

Phone cannot authenticate the CTL file.

Cause

The security token that signed the updated CTL file does not exist in the CTL file on the phone.

Solution

Change the security token in the CTL file and install the new file on the phone.

CTL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

Phone cannot authenticate any configuration files other than the CTL file.

Cause

A bad TFTP record exists, or the configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution

Check the TFTP record and the certificate in the Trust List.

ITL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

Phone cannot authenticate any configuration files other than the ITL file.

Cause

The configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution

Re-sign the configuration file by using the correct certificate.

TFTP Authorization Fails

Problem

Phone reports TFTP authorization failure.

Cause

The TFTP address for the phone does not exist in the CTL file.

If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.

Solution

Check the configuration of the TFTP address in the phone CTL file.

Phone Does Not Register

Problem

Phone does not register with Cisco Unified Communications Manager.

Cause

The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.

Solution

Change the Cisco Unified Communications Manager server information in the CTL file.

Signed Configuration Files Are Not Requested

Problem

Phone does not request signed configuration files.

Cause

The CTL file does not contain any TFTP entries with certificates.

Solution

Configure TFTP entries with certificates in the CTL file.

802.1X Authentication Problems

801.1X authentication problems can be broken into the categories that are described in the following table.

Table 42: 802.1X Authentication Problem Identification

If all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays `Configuring IP` or `Registering`. • 802.1X Authentication Status displays `Held`. • Status menu 802.1X status displays `Failed`.	802.1X Enabled on Phone but Phone Does Not Authenticate, on page 256

If all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays `Configuring IP` or `Registering`. • 802.1X Authentication Status displays `Disabled`. • Status menu displays that the DHCP status has timed out.	802.1X Not Enabled, on page 256
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status display as `Configuring IP` or `Registering`. • You are unable to access phone menus to verify 802.1X status.	Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 257

802.1X Enabled on Phone but Phone Does Not Authenticate

Problem

The phone cannot authenticate.

Cause

These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

Solution

To resolve this problem, check the 802.1X and shared secret configuration. See Identify 802.1X Authentication Problems, on page 261.

802.1X Not Enabled

Problem

The phone does not have 802.1X configured.

Cause

These errors typically indicate that 802.1X authentication is not enabled on the phone.

Solution

If 802.1X is not enabled on the phone, see 802.1X Authentication section.

Factory Reset of Phone Has Deleted 802.1X Shared Secret

Problem

After a reset, the phone does not authenticate.

Cause

These errors typically indicate that the phone has completed a factory reset while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

Solution

To resolve this situation, temporarily move the phone to a network environment that is not using 802.1X authentication. After the phone starts up normally, access the 802.1X configuration menus to enable device authentication and to reenter the shared secret. See 802.1X Authentication section for details.

Related Topics

Basic Reset, on page 263

General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

Phone Call Cannot Be Established

Problem

A user complains about not being able to make a call.

Cause

The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager. Phones with an LCD display show the message `Configuring IP` or `Registering`. Phones without an LCD display play the reorder tone (instead of dial tone) in the handset when the user attempts to make a call.

Solution

1 Verify the following:

   a The Ethernet cable is attached.
   b The Cisco CallManager service is running on the Cisco Unified Communications Manager server.
   c Both phones are registered to the same Cisco Unified Communications Manager.

2 Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem

The user complains that numbers are missed or delayed when the keypad is used.

Cause

Pressing the keys too quickly can result in missed or delayed digits.

Solution

Keys should not be pressed rapidly.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Check TFTP Settings

Procedure

Step 1 You can determine the IP address of the TFTP server that the phone uses by pressing **Applications**, then selecting **Administrator Settings** > **Network Setup** > **IPv4 Setup** > **TFTP Server 1**.

Step 2 If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option.

Step 3 If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.

Step 4 You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone recently moved from one location to another.

Step 5 If the local DHCP does not offer the correct TFTP address, enable the phone to use an alternate TFTP server. This is often necessary in VPN scenario.

Related Topics

Phone Cannot Connect to TFTP Server, on page 248

Determine DNS or Connectivity Issues

Procedure

Step 1 Use the Reset Settings menu to reset phone settings to their default values.

Step 2 Modify DHCP and IP settings:

a) Disable DHCP.

b) Assign static IP values to the phone. Use the same default router setting that other functioning Cisco IP Phones use.

c) Assign a TFTP server. Use the same TFTP server that other functioning Cisco IP Phones use.

Step 3 On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4 From Cisco Unified Communications Manager, choose **System** > **Server** and verify that reference to the server is made by the IP address and not by the DNS name.

Step 5 From Cisco Unified Communications Manager, choose **Device** > **Phone**. Click **Find** to search for this phone. Verify that you have assigned the correct MAC address to this Cisco IP Phone.

Step 6 Power cycle the phone.

Related Topics

Basic Reset, on page 263
Determine Phone MAC Address, on page 70

Check DHCP Settings

Procedure

Step 1 On the Cisco IP Phone, press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **IPv4 Setup**, and look at the following options:

- DHCP Server: If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If no value is found, check your IP routing and VLAN configuration. See the *Troubleshooting Switch Port and Interface Problems* document, available at this URL:

  http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

- IP Address, Subnet Mask, Default Router: If you have assigned a static IP address to the phone, you must manually enter settings for these options.

Step 3 If you are using DHCP, check the IP addresses that your DHCP server distributes.
See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Related Topics

Phone Cannot Connect to Server, on page 249
Phone Resets Due to DHCP Setting Errors, on page 251

Create New Phone Configuration File

Note

- When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the *Cisco Unified Communications Manager Administration Guide* for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

To create a new configuration file, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device** > **Phone** and click **Find** to locate the phone that is experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Note When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the *Cisco Unified Communications Manager Administration Guide* for more information.

Step 3 Add the phone back to the Cisco Unified Communications Manager database.

Step 4 Power cycle the phone.

Related Topics

Phone Addition Methods, on page 71

Identify 802.1X Authentication Problems

Procedure

Step 1 Verify that you have properly configured the required components.

Step 2 Confirm that the shared secret is configured on the phone.

- If the shared secret is configured, verify that you have the same shared secret on the authentication server.
- If the shared secret is not configured on the phone, enter it, and ensure that it matches the shared secret on the authentication server.

Verify DNS Settings

To verify DNS settings, follow these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **IPv4 Setup** > **DNS Server 1**.

Step 3 You should also verify that a CNAME entry was made in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.
You must also ensure that DNS is configured to do reverse lookups.

Start Service

Note A service must be activated before it can be started or stopped.

To start a service, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

Step 2 Choose **Tools** > **Control Center - Feature Services**.

Step 3 Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

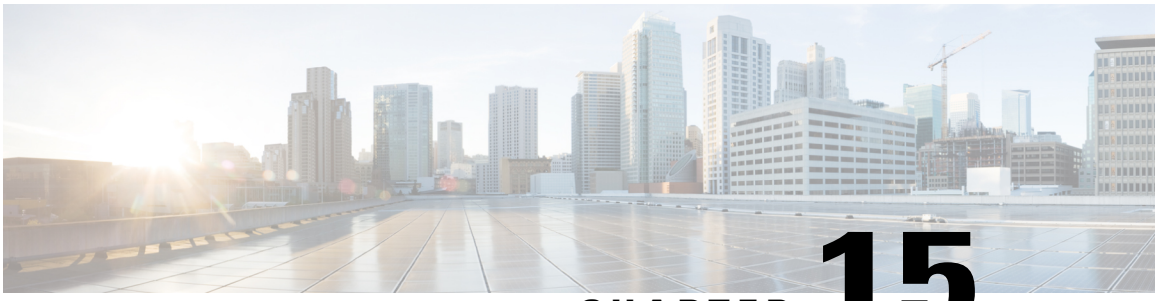
The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

Step 4 If a service has stopped, click the corresponding radio button and then click **Start**.
The Service Status symbol changes from a square to an arrow.

Additional Troubleshooting Information

If you have additional questions about troubleshooting your phone, go to the following Cisco website and navigate to the desired phone model:

http://www.cisco.com/cisco/web/psa/troubleshoot.html



CHAPTER 15

Maintenance

- Basic Reset, page 263
- Perform Network Configuration Reset, page 265
- Perform User Network Configuration Reset, page 265
- Remove CTL File, page 265
- Quality Report Tool, page 266
- Voice Quality Monitoring, page 266
- Cisco IP Phone Cleaning, page 267

Basic Reset

Performing a basic reset of a Cisco IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

The following table describes the ways to perform a basic reset. You can reset a phone with any of these operations after the phone has started up. Choose the operation that is appropriate for your situation.

Table 43: Basic Reset Methods

Operation	Action	Explanation
Restart phone	Press **Services, Applications, or Directories** and then press **#**.	Resets any user and network setup changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings, then restarts the phone.

Operation	Action	Explanation
Reset settings	To reset settings, press **Applications** and choose **Administrator Settings** > **Reset Settings** > **Network**.	Resets user and network setup settings to their default values, and restarts the phone.
	To reset the CTL file, press **Applications** and choose **Administrator Settings** > **Reset Settings** > **Security**.	Resets the CTL file.

Perform Factory Reset from Phone Keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

Procedure

Step 1 Unplug the phone:

- If using PoE, unplug the LAN cable.
- If using the power cube, unplug the power cube.

Step 2 Wait 5 seconds.

Step 3 Press and hold **#** and plug the phone back in.

Step 4 When the light on the Mute button turns off and all other lights stay green, press **123456789*0#** in sequence. After you press these buttons, the phone goes through the factory reset process.

Caution Do not power down the phone until it completes the factory reset process, and the main screen appears.

Perform Factory Reset Phone Menu

To perform a factory reset of a phone,

Procedure

Step 1 Press **Applications**.

Step 2 Choose **Administrator Settings** > **Reset Settings** > **All**.
If required, unlock the phone options.

Related Topics

Apply Phone Password, on page 45

Perform Network Configuration Reset

Resets network configuration settings to their default values and resets the phone. This method causes DHCP to reconfigure the IP address of the phone.

Procedure

Step 1 From the Administrator Settings menu, if required, unlock phone options.

Step 2 Choose **Reset Settings** > **Network Setup**.

Related Topics

Apply Phone Password, on page 45

Perform User Network Configuration Reset

Resets any user and network configuration changes that you have made, but that the phone has not written to flash memory, to previously saved settings.

Procedure

Step 1 From the Administrator Settings menu, if required, unlock phone options.

Step 2 Choose **Reset Settings** > **Reset Device**.

Related Topics

Apply Phone Password, on page 45

Remove CTL File

Deletes only the CTL file from the phone.

Procedure

Step 1 From the Administrator Settings menu, if required, unlock phone options.

Step 2 Choose **Reset Settings** > **Security Settings**.

Related Topics

Apply Phone Password, on page 45

Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco IP Phone. The QRT feature is installed as part of Cisco Unified Communications Manager installation.

You can configure user Cisco IP Phones with QRT. When you do so, users can report problems with phone calls by pressing Report Quality. This softkey or button is available only when the Cisco IP Phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses Report Quality, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information that is logged depends on the user selection and whether the destination device is a Cisco IP Phone.

For more information about using QRT, see *Cisco Unified Communications Manager Features and Services Guide*.

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics: Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics: Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.

Note Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

Table 44: Changes to Voice Quality Metrics

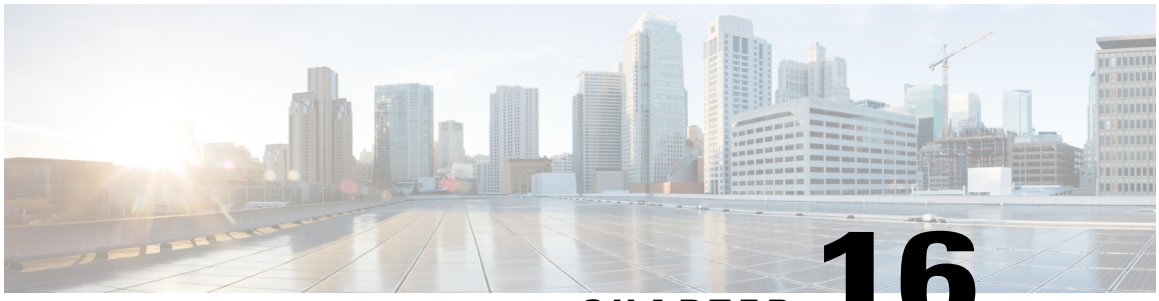
Metric change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter levels: • Average MOS LQK decreases may indicate widespread and uniform impairment. • Individual MOS LQK decreases may indicate bursty impairment. Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.
MOS LQK scores increase significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

Note Voice quality metrics do not account for noise or distortion, only frame loss.

Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.



CHAPTER 16

International User Support

- Unified Communications Manager Endpoints Locale Installer, page 269
- International Call Logging Support, page 269

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the "Locale Installer" section in the *Cisco Unified Communications Operating System Administration Guide*.

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.